

ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ



как мошенники
обманывают
детей в интернете

Совет №1

Научите ребёнка правилам безопасности для виртуальных покупок

Не переходить по ссылкам на незнакомые сайты.

Не вводить на незнакомых сайтах пароли от игр, соцсетей, реквизиты карты и коды из sms.

Покупать виртуальные
товары только
в официальных приложениях.

Не оплачивать покупки через
боты в соцсетях.



Фейковые сайты онлайн-покупок

Мошенники создают поддельные сайты продажи
виртуального инвентаря для онлайн-игр:
персонажей, одежду, предметов и т.п.

Если ввести на таком сайте
реквизиты карты, то можно
потерять деньги.

А если ввести пароль своего
игрового аккаунта или соцсети,
то мошенники и их могут украсть.



Совет №2

Объясните детям, что обещания лёгких денег — это всегда тревожный знак

Если ребёнку необходимы деньги на покупку дорогой вещи, то расскажите ему, как он может сам накопить нужную сумму.

Если копить придется долго, посоветуйте положить деньги на вклад или накопительный счёт, чтобы получать проценты на свои сбережения.



Лёгкий заработка

Мошенники могут предложить детям оставлять комментарии под постами блогеров за вознаграждение или писать платные отзывы о товарах.

Для вывода «заработка» аферисты просят оплатить комиссию, введя на их сайте реквизиты карты.

В итоге деньги вместе с данными карты оказываются в руках преступников.



Совет №3

Поговорите с подростком об опасностях дропперства

Нельзя никому передавать свою карту
или её реквизиты.

Если незнакомец прислал ребёнку
деньги якобы «по ошибке»

и просит перевести их,
этого делать нельзя!

Родители должны обратиться
в банк, чтобы тот вернул
сумму отправителю.

За дропперство предусмотрена
уголовная ответственность!



Вовлечение в дропперство

Мошенники переводят похищенные у других людей
деньги на счета школьников, а затем просят
за вознаграждение обналичить их
или перевести сообщникам.

Такие промежуточные счета
называют дропперскими,
а самих посредников –
дропперами.

Часто подростки даже
не подозревают, что
помогают мошенникам.



Совет №4

Помогите ребёнку усвоить правила кибергигиены

Прежде чем выполнять просьбы «друга», лучше позвонить ему. Скорее всего, он не в курсе переписки.

Защититься от вредоносных ссылок помогут антивирусные приложения. Не забывайте обновлять их.

Для безопасности маленьких детей можно настроить программы родительского контроля.



Просьбы о помощи от имени друзей

Мошенники взламывают аккаунты в соцсетях и рассылают по списку друзей просьбы срочно одолжить денег.

Или пишут «лови свои фотки!», но вместо ссылки на фото присылают вирус, который крадет с гаджета логины, пароли и коды оплаты из sms.



Вывод денег с Пушкинской карты

Мошенники продают в соцсетях «инструкции»
по обналичиванию денег с Пушкинской карты.
На самом деле это невозможно.

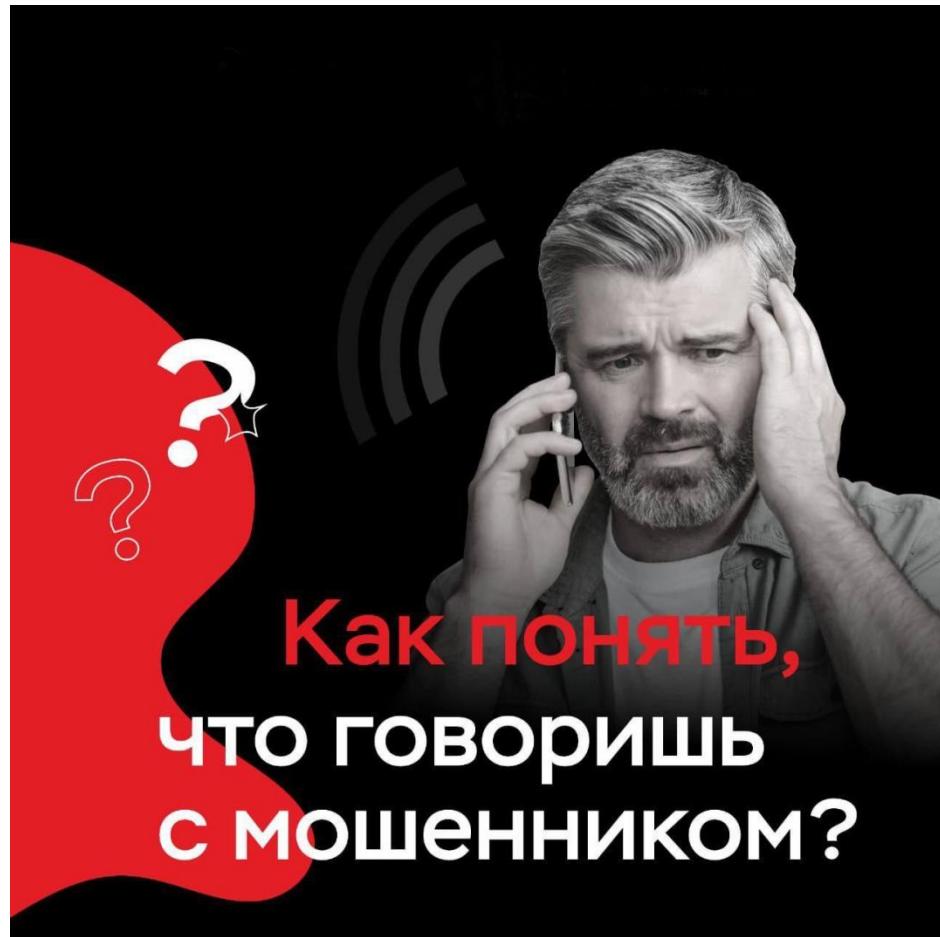
Обычно такая «инструкция»
стоит порядка 100 рублей.

Мошенники просто
прикарманяют эти деньги.

— Ах, обмануть меня
не трудно, я сам
обманываться рад...



ОБРАЗ МОШЕННИКА



**Как понять,
что говоришь
с мошенником?**



Образ мошенника:

“сотрудник Соцфонда”

- предлагает получить единовременную выплату
- настаивает на пересчете пенсии



7

Образ мошенника:

“оператор мобильной связи”

- 
- сообщает о смене тарифного плана
 - пугает отключением услуг
 - предлагает переоформить договор

6

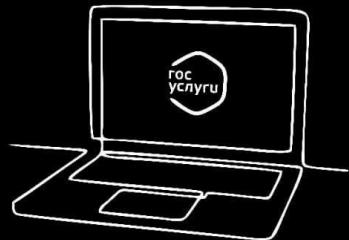


Образ мошенника:

“сотрудник полиции”

- ведет расследование об утечке персональных данных
- просит помочи в задержании аферистов
- обвиняет в госизмене

4



Образ мошенника:

“служба безопасности Госуслуг”

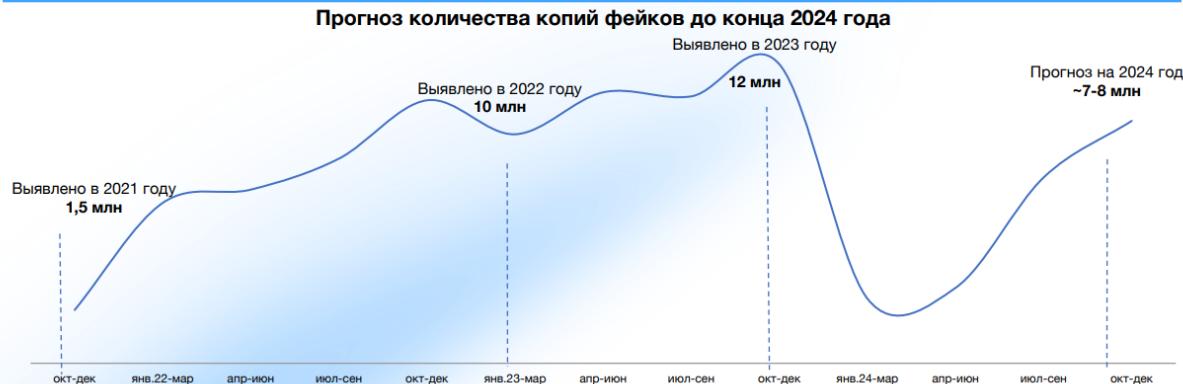
- пугает взломом личного кабинета
- сообщает о попытке оформить онлайн-кредит
- говорит об утечке персональных данных

5

ПРОТИВОДЕЙСТВИЕ ФЕЙКАМ

Фейков становится больше в кризисные моменты

Несмотря на прогнозы, фиксируется снижение количества фейков в 2024 г.



ПРИЧИНЫ:

- Усталость пользователей от фейков по СВО
- Рост доли региональных кейсов
- Повышение оперативности мер противодействия
- Сокращение жизненного цикла фейка

За первое полугодие количество **копий уменьшилось на 44%** по сравнению с аналогичным периодом 2023 г., при снижении количества уникальных фейков на 3%

МЕХАНИЗМЫ ПРОВЕДЕНИЯ ИНФОРМАЦИОННЫХ АТАК

Закупка таргетированной рекламы

Создание «спящих» ТГ-каналов, позиционирующихся как российские

Атаки на российские компании и органы власти:

- Взлом сайтов и интернет-порталов.
- Хакерские атаки
- DDoS-атаки на сайты компаний (аптеки, интернет-площадки и тд).
- Создание фейковых сайтов (государственных ресурсов и пр.)
- Взлом баз данных.

Фейковые аккаунты российских СМИ и государственных органов

Выявление контактных данных родственников военных

Фейковые аккаунты для распространения недостоверной информации среди граждан РФ

Участие известных украинских и оппозиционных блогеров

РАСПРОСТРАНЕНИЕ ФЕЙКОВ



РОСТ КОЛИЧЕСТВА ФЕЙКОВ В РЕГИОНАХ

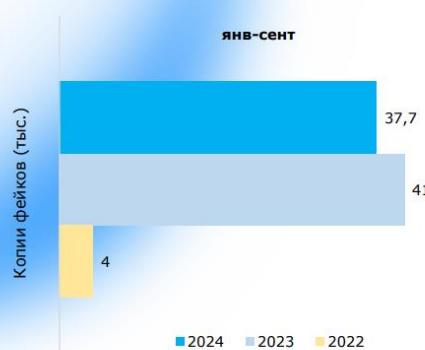


МЕЖНАЦИОНАЛЬНАЯ РОЗНЬ

Угрозы от фейков:

- Способствуют разжиганию ненависти и вражды
- Усиливают стереотипы и предубеждения
- Способствуют созданию атмосферы страха и подозрительности
- Воздействуют на общественное мнение
- Усиливают экстремизм
- Разрушают социальную сплоченность

Фейки о межнациональных отношениях (2022-2024 гг.)



ФЕЙК – СВЕРХФАКТОР РИСКА

ДЛЯ ГОСУДАРСТВА И ОИВ

- Дестабилизация социально-политической ситуации (митинги, протесты, гибель людей и пр.)
- Формирование негативного имиджа лица или организации

ДЛЯ СМИ И МЕДИА

- Правовые последствия
- Утрата доверия пользователей
- Социальная ответственность

ЛИЧНО ДЛЯ ВАС

- Потеря материальных ценностей
- Смена моральных установок
- Повышение тревожности

МАРКЕРЫ ФЕЙКА

- ✓ Эмоции: фактор страха/опасности
- ✓ Лжефакты и тезисы
- ✓ Указание важности или срочности
- ✓ Ссылка на «достоверный» источник
- ✓ Утверждение достоверности
- ✓ Геопривязка
- ✓ Призыв к распространению
- ✓ Призыв к действию или бездействию
- ✓ Лингвистические конструкции «раскрытия правды» и «перекладывания ответственности»



КЛЮЧЕВЫЕ ЭТАПЫ РАБОТЫ С ФЕЙКОМ

1

2

3

4

5

ВЫЯВЛЕНИЕ

ВЫБОР СТРАТЕГИИ

ОЦЕНКА И КОНТРОЛЬ

ВЕРИФИКАЦИЯ

ОПРОВЕРЖЕНИЕ

ОЦЕНКА ПРИНЯТИЯ РЕШЕНИЯ

Перед началом работы по опровержению необходимо ответить на 3 пункта:

- 1** Какой у фейка охват и аудитория? Локальный канал или крупнейшее СМИ?
- 2** Хватает ли доказательств для разоблачения? Или это просто «слово против слова»?
- 3** Стоит ли трогать эту тему? Не создадите ли эффект Стрейзанд?

КОМПОНЕНТЫ ОПРОВЕРЖЕНИЯ



ИНФОРМАЦИОННО-СПРАВОЧНЫЕ МАТЕРИАЛЫ ПО ВОПРОСАМ ПРОТИВОДЕЙСТВИЯ НEDОСТОВЕРНОЙ (ФЕЙКОВОЙ) ИНФОРМАЦИИ

ДЛЯ ИСПОЛЬЗОВАНИЯ В РАБОТЕ ПО ЗАЩИТЕ КАДРОВОГО СОСТАВА
ОТ НЕГАТИВНОГО ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

**ПРОФИЛАКТИКА КИБЕРУГРОЗ:
КАК НЕ СТАТЬ ЖЕРТВОЙ
ТЕХНОЛОГИЙ И ИНФОРМАЦИИ**



ОГЛАВЛЕНИЕ

★ Предисловие	03
★ Проверка данных (Фактчекинг)	04
★ Фейки и как их определить	05
★ Признаки фейковых рассылок	06
★ Что такое дипфейк	07
★ Примеры дипфейков	08
★ ИНТЕРНЕТ-МОШЕННИЧЕСТВО И КИБЕРБЕЗОПАСНОСТЬ	09
★ Кражи личных данных (Фишинг)	10
★ Атаки на Интернет-вещей (IoT-устройства)	11
★ Эксплуатация уязвимостей	12
★ Атаки через социальную инженерию	13
★ Атаки через искусственный интеллект (ИИ)	14
★ Выводы	15

ПРЕДИСЛОВИЕ

В условиях стремительного развития технологий и цифровизации нашей жизни кибермошенничество становится одной из самых значимых угроз современного общества. С ростом использования онлайн-сервисов и мобильных приложений не только люди становятся более уязвимыми для манипуляций и атак, но и государственные и частные компании.

По данным Следственного департамента МВД, за первые семь месяцев 2024 года зарегистрировано 577 000 IT-преступлений, из них 437 000 – это мошенничество и хищения. Ущерб от таких преступлений оценивается в 99 млрд руб.

По данным Банка России, в I квартале 2024 года количество мошеннических операций выросло почти на 17%. За этот период злоумышленникам удалось похитить у клиентов банков 4,3 млрд рублей. Наибольший объем хищений зафиксирован через банковские карты – 1,9 млрд руб. Если в прошлые годы большинство операций без согласия клиентов приходилось на оплату товаров и услуг в Интернете, в последнее время злоумышленники сфокусировались на дистанционных банковских сервисах. Мошенники не только похищают у человека средства со счета, но и оформляют на него кредит.

Не менее серьезной угрозой становятся и фейковые (ложные) новости, которые распространяются через социальные сети, мессенджеры и другие цифровые платформы. Ложная информация может привести не только к материальному ущербу, но и к разрушению общественного доверия, дестабилизации политической ситуации и социальной напряженности. Фейковые новости часто используются для манипуляции мнением граждан, создания паники или разжигания конфликтов. Согласно данным социологического IT-центра «Диалог», число фейков, сгенерированных нейросетью, выросло почти на 75% за 2024 год по сравнению с аналогичным периодом.

Раскрываемость киберпреступлений остается стабильно низкой и не превышает 27%. В этих условиях недостаточно рассчитывать на усилия правоохранительных органов – нужно активно повышать осведомленность граждан о киберугрозах. В памятке собрана информация о самых распространенных на сегодняшний день видах онлайн-мошенничества, а также простые и эффективные способы борьбы с ними.

ЧТО ТАКОЕ ФАКТЧЕКИНГ



Это процесс проверки информации на достоверность, фактическую точность



<p>Поиск и анализ первоисточника</p> <p>Не доверяйте репостам. Источник информации должен быть авторитетным и надежным</p>	<p>Правило нескольких источников</p> <p>Даже если первоисточник надежный, сравните эти данные с разными источниками</p>	<p>Проверка цитирования</p> <p>Цитирование должно быть точным, полным, не вырванным из контекста</p>
<p>Анализ контекста</p> <p>Иногда данные могут быть истинными в одном контексте и ложными в другом. Изучите обстоятельства, в которых была получена информация</p>	<p>Проверка фото и видео</p> <p>Используйте обратный поиск изображений для определения даты первоначального размещения</p>	<p>Проверка статистических данных</p> <p>Данные должны быть подтверждены достоверными источниками и правильно интерпретироваться</p>
<p>Оценка стиля письма</p> <p>Наличие ярких эмоциональных утверждений в тексте публикаций может указывать на недостоверную информацию</p>	<p>Проверка даты публикации</p> <p>Информация должна быть актуальной и неустаревшей</p>	<p>Оценка заголовков и содержания</p> <p>Заголовки могут быть утрированными или слишком эмоциональными. Читайте статью целиком для получения достоверной информации</p>
<p>Исключение подтасованных данных</p> <p>Информация не должна быть манипулятивной или представлять только одну точку зрения</p>	<p>Проверка качества ссылок</p> <p>Все ссылки должны вести на надежные и авторитетные источники</p>	<p>Внимательность к анонимным источникам</p> <p>Информация может быть менее достоверной или представлять интересы определенной стороны</p>

ФЕЙКИ И КАК ИХ ОПРЕДЕЛИТЬ



Фейки — заведомо недостоверная, сфальсифицированная информация, призванная ввести в заблуждение. Маркеры фейка в публикациях не всегда подтверждают ложность информации, но указывают на необходимость более тщательной проверки сообщения.

Самые распространенные маркеры

Информация вызывает сильные эмоции: испуг, страх, возмущение

“

Предсказан конец света!

Прогнозирование событий по катастрофическому сценарию

“

Коронавирусом переболеет 90% населения земного шара

Анонимная подача информации от якобы авторитетного лица

“

Близкий к руководству человек сказал...

Конспирологическая аргументация (ссылка на некий заговор)

“

Десятилетиями от нас скрывали... Тот самый запретный выпуск

Предоставление оценочных суждений, выгодных автору, без подтверждения

“

Опросы показывают высокий уровень поддержки N

Оценка текущих событий с точки зрения широкого исторического контекста

“

Россия всегда была агрессивным государством

Использование догадок и домыслов в качестве аргументов

Это любые возможные, но не доказанные факты и события

Наличие в тексте ошибок

Это могут быть опечатки, пунктуационные и речевые ошибки, наличие сленговых и жаргонных выражений

Фейковые сообщения в мессенджерах

Характерные особенности

01

Не имеют авторства и ссылки на конкретный ресурс (в отличие от фейков в СМИ)

02

Имеют целью получить большой охват аудитории, мотивируют к частой пересылке

03

Эмоциональны, обращены «лично» к адресату

04

Содержат недостоверную информацию и часто орфографические ошибки

05

Привязаны к актуальным событиям в обществе

06

Негативны по содержанию, сеют панику



Типичные признаки фейковых рассылок

	Написание заголовков и предложений прописными буквами с обилием восклицательных знаков	«ПРЕДУПРЕЖДЕНИЕ», «МАКСИМАЛЬНЫЙ РЕПОСТ!!», «РАСПРОСТРАНИТЬ СРОЧНО! ВО ВСЕХ СЕТЯХ!!!!»
	Использование эмодзи, специальных значков, идеограмм и смайликов, характерных для сообщений и переписки в мессенджерах	«СРОЧНО !!!»
	Прямое обращение к адресату по профессии или роду деятельности, а также эмоциональные прилагательные, которые сокращают дистанцию между автором и читателем	«Родные мои!», «Братья и сестры!», «Коллеги, друзья! Эта памятка для ВАС»
	Опечатки, пунктуационные, орфографические, речевые ошибки	Вероятно, автор послания сознательно имитирует речь простого человека.. Важно помнить, в официальных текстах ошибки не допускаются
	Использование лексики, касающейся базовых ценностей: здоровье, безопасность, жизнь, питание, жилище, дети, деньги	«И тогда не нужны уже будут нам ни сотовые, ни квартиры, ни образование детям, ни машины, ни отдых комфорtabельный за границей»
	Ложная ссылка на авторитетные источники	«Только представьте себе, о чём в «колокола бьют» не только старец Илия, но и Афонские старцы», «Источник: ГЕРМАНИЯ, Министерство здравоохранения»
	Прогнозирование развития событий по катастрофическому сценарию	«Вот-вот все рванет, и извне, но более опасен для России всегда был враг внутренний»
	Использование эмоциональной лексики, давление на человеческие чувства, морализаторство	«Не будьте безразличны, не отмахивайтесь...», «ПОДЕЛИТЕСЬ, ЧТОБ ВЕСЬ МИР ЗНАЛ!»
	Настойчивый призыв к действию и распространению информации	«Передайте это своей семье, всем соседям, знакомым, друзьям, коллегам»

БАЗОВАЯ ПРОВЕРКА ИЗОБРАЖЕНИЙ



Подозрительное фото/видео можно проверить с помощью сервиса «Яндекс.Картинки». Так вы определите, как давно изображение появилось в сети, найдете оригинал, обрезанные и необрезанные версии. Возможно, окажется, что картинка стоковая — это тоже признак фейка

ЧТО ТАКОЕ ДИПФЕЙК



Дипфейк (Deepfake)

Это технология, основанная на искусственном интеллекте, которая позволяет создавать фальшивые медиафайлы, заменяя на видео лица или манипулируя изображениями таким образом, что результат выглядит вполне правдоподобно

Категории дипфейков

01

Генерация текста и визуального контента с использованием нейросетей

02

Дипфейки в реальном времени

03

Спупинг. Нейросети могут «клонировать» голос любого человека на основе аудиозаписей этого голоса

04

Фальшивые аккаунты. Алгоритмы ИИ могут быть использованы для создания поддельных профилей в интернете

Отличительные особенности дипфейков



Видеоконтент

Неестественные движения глаз. Например, нерегулярное моргание

Несинхронные или резкие движения различных частей тела



Рассинхронизация движения губ с произносимой речью

Смещение яркости на разных кадрах

Несоответствие цвета лица и остальных частей тела



Фотографии

Нейросетям еще не удается повысить качество прорисовки пальцев рук (например, шесть пальцев или их отсутствие)

Если на картинке видны зубы, стоит присмотреться. Аналогично прорисовке пальцев нейросетью



Аудиозапись

Резкая, неестественная смена интонаций

Отсутствие окончаний слов и предложений

Односложные, излишне простые предложения. Например, нетипичная речь у политиков, которые обычно любят «извилистые» конструкции



РАСПРОСТРАНЕННЫЕ ПРИМЕРЫ ДИПФЕЙКОВ



Фейк

Жителям Курской области необходимо приготовиться к эвакуации, которая может начаться в ближайшее время. В Сети распространяется видео врио губернатора Курской области Алексея Смирнова

Ссылка на фейк

https://t.me/kursk_v_teme/103

Опровержение

За основу взято реальное выступление врио губернатора Курской области, которое он опубликовал у себя в официальном телеграм-канале. Подделку выдают неестественные движения губ и монотонный «механический» голос

Исходное видео

https://t.me/governator_46/7235

Внимание, покупатели посёлка Коренево!

Сообщаем Вам, что с 9 августа 2024 года закоз продуктов и других товаров будет осуществляться раз в неделю - ни вторникам. Это связано с последними событиями в нашем районе. В целях Вашей безопасности просим:

- не создавать столпотворение
- не стоять на открытой местности
- заранее планируйте покупку

Берегите себя и своих близких с уважением администрации магазина!

Фейк

В соцсетях появилась фотография объявления, якобы размещенного в магазине в поселке Коренево. В нем сказано, что купить продукты можно будет теперь лишь в определенные дни

Опровержение

По данному фото невозможно распознать реальное расположение объявления — нет ни названия магазина, ни каких-то узнаваемых объектов. Официальные источники — власти поселка и региона — не сообщали о проблемах с поставкой продовольствия. Все магазины работают штатно



Фейк

В Белгороде по радио прозвучала воздушная тревога, людей предупреждают об опасности и просят спрятаться в укрытии. В конце сообщения говорится: «Скоро вы будете демилитаризованы. БНР будет свободной»

Ссылка на фейк

<https://t.me/uniannet/141331>

Опровержение

На видео наложена звуковая дорожка, что выдает несколько нюансов. Прежде всего, это начитка, выполненная с помощью нейросети. Это можно понять по характерной для искусственного интеллекта «ненжевой дикции» и соответствующим смысловым и интонационным ударениями. Текст, который звучит в ролике, избыточный и излишне эмоциональный

Видео опровержение

<https://t.me/beladm31/18359>



На данном слайде представлены примеры заведомо ложной информации и иллюстраций, распространяемых с целью введения в заблуждение, нагнетания паники и негативных настроений у граждан

ИНТЕРНЕТ-МОШЕННИЧЕСТВО И КИБЕРБЕЗОПАСНОСТЬ

Интернет делает нашу жизнь более уязвимой. Одна из актуальных угроз — онлайн-мошенники. Чтобы не стать их жертвой, нужно знать, какие киберпреступления сегодня распространены.

ВИДЫ СОВРЕМЕННОГО КИБЕРМОШЕННИЧЕСТВА

!
Фишинг

!
Атаки на Интернет вещей (IoT-устройства)

!
Эксплуатация уязвимостей

!
Атаки через социальную инженерию

!
Атаки через искусственный интеллект (ИИ)





Фишинг

Кража личных данных, например логинов и паролей, через поддельные веб-сайты или электронные письма.

Способы защиты

01

Использовать программы для фильтрации спама

02

Следить за тем, на какую кнопку нажимаете и по какой ссылке переходите

03

Проверять, корректно ли выглядит адрес сайта или электронное письмо

Примеры



Как проверить адрес сайта

Допустим, вы хотите зайти на сайт [vk](https://vk.com). Вбиваем запрос в поисковую строку браузера и смотрим результат выдачи

01

Проверяем адрес сайта. Он должен выглядеть именно так, и никак иначе <https://vk.com>!

02

Смотрим, есть ли логотип и описание у сайта

! Важно !

Страйтесь посещать сайты с защищенным протоколом [https](https://).

S значит «secure» — «безопасность»

03

Обращайте внимание, что компании зачастую берут короткое доменное имя, а также выкупают все похожие

Если видите длинное название типа <https://vk.site.safe.com>, то лучше усерднее его проверить



Мошенники могут использовать и короткий домен, например <https://vk.org>. Это ссылка на сайт-зеркало, который от официального отличается только окончанием домена



Как проверить электронное письмо

01

Нужно оценить содержание письма и проверить, за кем закреплен почтовый адрес отправителя. Если в письме есть слова: «На ваш счет зачислен выигрыш», «Заработайте без вложений» и похожие — это мошенники!

02

Также следует поискать сайт компании и узнать, указана ли там данная почта в качестве официальной



! Внимание !

Часто подделывают сайты маркетплейсов, к примеру Wildberries. После оформления заказа мошенники просят покупателя продолжить диалог в каком-нибудь мессенджере и переплатить деньги на реквизиты карты. При этом на почту даже может прийти письмо «от Wildberries» о поступлении средств



Помните, это незаконно!

Все переписки, все транзакции должны происходить только на платформе маркетплейса. Если что-то пойдет не так, вы сможете обратиться в службу поддержки



Атаки на Интернет вещей (IoT-устройства)

Сеть устройств, которые оснащены средствами связи друг с другом — это **интернет-вещей (IoT-устройства, Internet of Things)**. Например системы безопасности дома, умные колонки, холодильники и другая бытовая техника. Такие устройства все чаще становятся мишенью для атак.

Способы защиты

01

Изолировать такие устройства в отдельную сеть с надежным паролем для доступа

02

Отслеживать, не подключились ли к вашей домашней сети посторонние устройства

03

Не использовать общедоступную сеть Wi-Fi и тем более не пересыпать с помощью нее важные данные

04

Если нет возможности подключиться к домашней сети Wi-Fi, использовать мобильный интернет

Пример



Человек подключился к сети Wi-Fi в кафе

Зашел в аккаунт своего банка и произвел некую операцию. После злоумышленник подключился к той же сети и перехватил все доступы — теперь деньги в руках мошенника

! Важно

Если подключения к общей сети Wi-Fi не избежать:

- 01 Заходите на сайты только с протоколом https
- 02 Настройте двухфакторную аутентификацию





Эксплуатация уязвимостей

Программное обеспечение постоянно обновляется. Старые версии становятся менее актуальными и более уязвимыми для мошеннических действий.

Способы защиты

01

Избегать старых версий программ: обновление — это усиление безопасности и удобства

02

Следить за регулярным обновлением и патчингом систем

03

Скачивать обновления для мобильных приложений из официальных магазинов (например, RuStore)

04

Следить, что вы разрешаете вашим приложениям. Лучше всего выбирать пункт «только при использовании приложения»

05

Использовать системы управления уязвимостями для мониторинга и устранения рисков



Атаки через социальную инженерию

Злоумышленники используют психологические приемы и манипулируют пользователями. Например, могут представиться сотрудниками банка или полиции для получения доступа к личным данным.

Способы защиты

01

Научиться распознавать тактики атак через социальную инженерию (обращение за экстренной помощью, предложения приобрести какой-то продукт или помочь разрешить «проблемную» ситуацию)



Некоторые приложения передают данные своих пользователей

Поэтому, прежде чем выбрать программу для определения спама, почитайте отзывы на разных источниках, посмотрите оценку приложения и обзоры от профессионалов

02

Соблюдать культуру безопасности: никому и никогда не сообщайте логины и пароли к личным аккаунтам, коды безопасности (CVC) банковских карт, не делитесь персональными данными и другой личной информацией с незнакомыми людьми, используйте программы определения спама

Примеры атак через социальную инженерию



Человеку поступил звонок от «сотрудников банка»

Просят назвать цифры с оборотной стороны карты. После чего снимают со счета все деньги



Звонок из «телефонной компании»

Просят назвать пароль аккаунта на «Госуслугах». Мошенник получает доступ к паспорту и справке 2-НДФЛ, а затем оформляет онлайн-кредит на имя жертвы



Звонок от «сотрудников» полиции

Они говорят жертве, что на нее заведено дело и предлагают от него откупиться

! Важно

В подобных ситуациях необходимо быть морально устойчивым к нападкам со стороны злоумышленников, делать паузы и анализировать, что вам говорят.

Мошенники пытаются действовать быстро, чтобы вы не успели обработать информацию и сделали то, что просят. Лучше всего просто положить трубку и перезвонить по официальным контактам организации, сотрудниками которой представились потенциальные мошенники. Если остались сомнения, обратитесь за советом к профессиональным юристам.



Идентификационные атаки

Кража идентификационных данных пользователей, например имени, домена, адреса электронной почты, пароля, цифровых сертификатов и т.п. В отличие от атак через социальную инженерию, персональные данные злоумышленники получают без вашей «помощи».

Способы защиты

01

Настроить двухфакторную аутентификацию

02

Регулярно обновлять пароли



Атаки через искусственный интеллект (ИИ)

Искусственный интеллект (ИИ) помогает мошенникам обходить защиту сайтов, обрабатывать большие объемы данных, создавать ботов, совершать спам-атаки и многое другое.



Дипфейк — один из самых распространенных способов атаки через ИИ



Вы можете получить звонок, в том числе видеозвонок, или видеосообщение

Фейк может выглядеть и говорить очень похоже на вашего друга или родственника. Мошенники также могут подделать номер телефона

Способы защиты

01

Если собеседник пытается узнать у вас конфиденциальную информацию, угрожает, завершите подозрительный звонок и перезвоните человеку по номеру, который сохранен у вас в телефоне

02

Придумайте кодовые фразы для разговора по телефону

03

Задайте неожиданный вопрос, ответ на который может знать только ваш настоящий собеседник. Это поможет понять, кто с вами разговаривает

04

Каждый раз ведите запись диалога, чтобы иметь доказательства мошенничества

05

Используйте инструменты и программы для распознавания дипфейков

06

Подмечайте неточности в видео, например в движениях губ или бровей

! Внимание

Дипфейк может имитировать даже представителей госструктур

Они будут сидеть в кабинете, в форме и озвучивать какие-то требования к вам. В такой ситуации лучше прекратить общение, а также проверить информацию с помощью достоверных источников: на официальных сайтах министерств и ведомств, от которых поступило подозрительное сообщение.



Выводы



Избегайте любой передачи важных данных через интернет

Только так можно быть в полной безопасности



Всегда будьте в «фокусе» и не теряйте концентрации

Обязательно включайте критическое мышление



Помните, что у государственных и финансовых организаций существуют каналы связи, установленные законом РФ

Обычно это электронная почта, почта России, специализированные платформы («Госуслуги»).

Поэтому, например, сотрудники МВД никогда не позвонят или не отправят различные уведомления/документы по WhatsApp* в рамках официального общения. На подобные звонки или сообщения вы вправе не отвечать.

*принадлежит компании Meta, которая признана в России экстремистской, ее деятельность запрещена

РАБОТА С ТЕЛЕГРАММ-АККАУНТОМ

Как обезопасить свой Телеграм-аккаунт



Как происходит взлом аккаунта?

Пользователю поступает уведомление от кого-то из списка контактов с подарочной подпиской на Telegram Premium. Пользователь кликает кнопку, чтобы получить подписку, после чего ему приходит код авторизации. На экране с подарком написано, что этот код необходимо ввести, чтобы активировать премиум-подписку. После активации кода аккаунт переходит в руки злоумышленника.



Подключите двухфакторную аутентификацию

Чтобы включить двухфакторную аутентификацию в Телеграм, нужно:

1. зайти в Настройки,
2. перейти в раздел «Конфиденциальность»,
3. выбрать «Облачный пароль», придумать пароль и запомнить его.

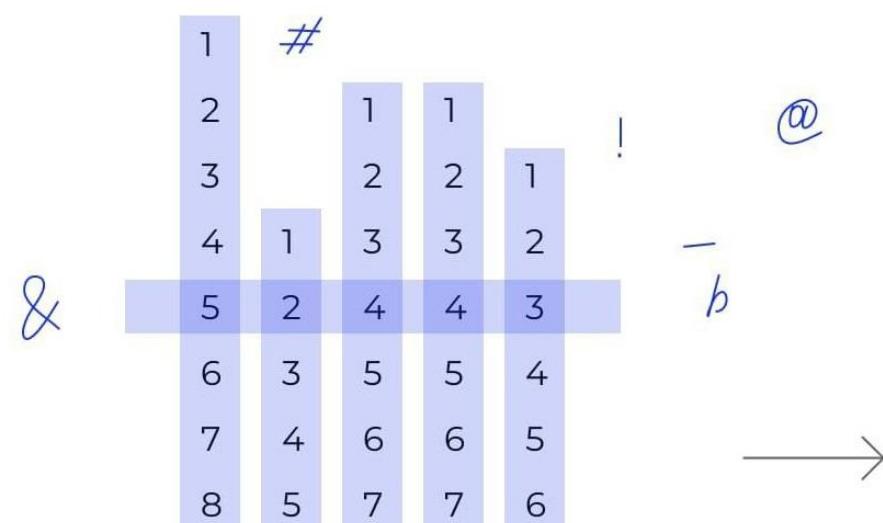


03

Подключите двухфакторную аутентификацию

Пароль может состоять из любого сочетания букв и/или цифр и содержать любое количество символов. Также Телеграм предложит указать адрес электронной почты. Если вы забудете пароль, можно будет сбросить его, перейдя по ссылке в письме, которое придет на указанную вами почту.

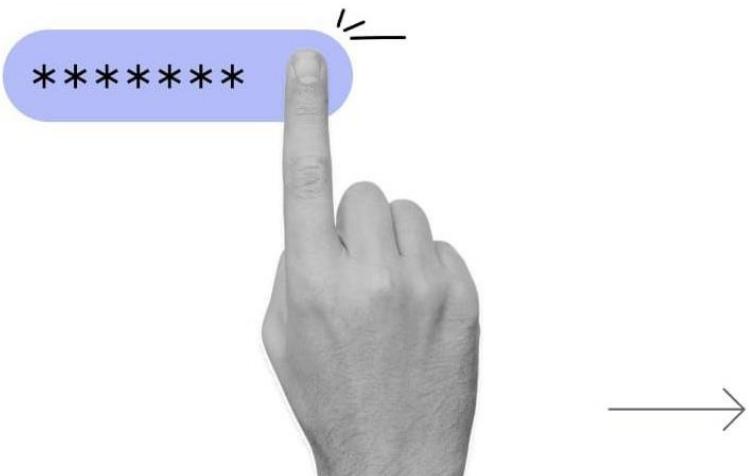
04



Установите дополнительный код-пароль

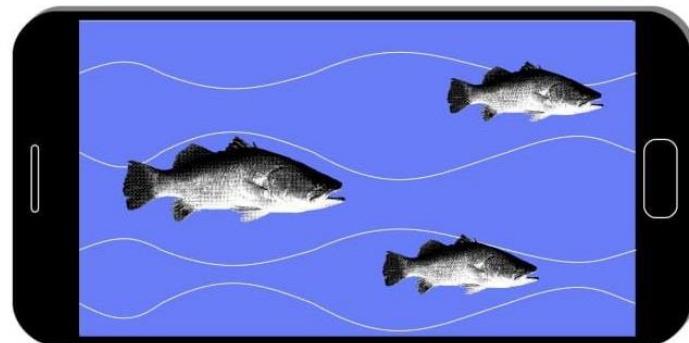
В Телеграм можно установить дополнительный пароль, который необходимо будет вводить каждый раз при входе в приложение. Можно выбрать разблокировку по отпечатку пальца, Face ID или код. Таким образом вы сможете дополнительно защитить аккаунт при входе с разных устройств.

05



Настройте видимость номера телефона

Найти человека в Телеграм можно двумя способами: зная его имя пользователя (индивидуальное имя, которое пользователь придумывает сам для себя, выделяется спереди знаком @) или номер телефона.



06



Настройте видимость номера телефона

По умолчанию в мессенджере ваш номер телефона виден всем, у кого он есть в телефонной книге, а также тем, чей номер записан у вас.

В разделе «Номер телефона» можно скрыть свой номер телефона от тех пользователей, кто записан у вас в телефонной книге, но не имеет вашего номера телефона.

07



Приглашение в группы и каналы

Зная номер телефона или имя, пользователь может добавить вас в любую группу или пригласить в любой телеграм-канал. Это удобная функция, если друзья хотят создать с вами общую группу или быть подписанными на один канал. Но таким образом ваш аккаунт распространяется по многим группам и его могут увидеть множество незнакомых вам пользователей.

В разделе «Группы и каналы» вы можете самостоятельно выбрать, кому разрешаете добавлять вас в группы или приглашать в каналы.

08