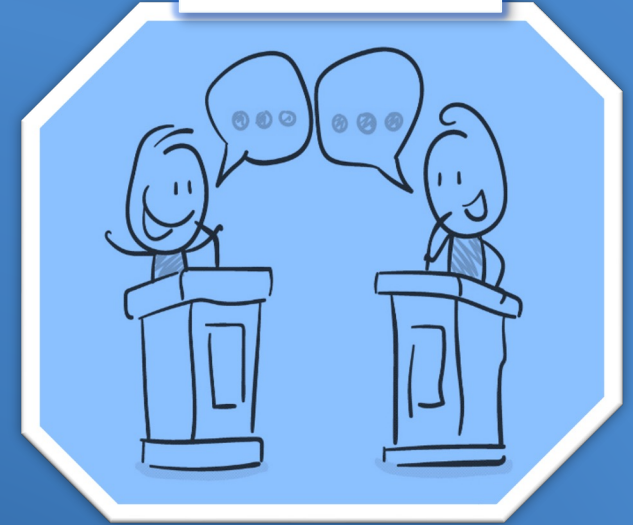




ПОМОЩЬ В ПОДГОТОВКЕ К ДЕБАТАМ

АРГУМЕНТАЦИЯ ПОДСКАЗКИ



Мошенники в цифровом мире

Персональные данные

Осторожно, финансовые пирамиды!

Логины и пароли



ТЕЗИС

Использование новых технологий оплаты и хранения данных важнее для защиты от мошенников, чем умение противостоять обману (методам социальной инженерии)

КОНТРЕЗИС

Новые технологии оплаты и хранения данных не защитят от мошенников, если не знаешь ключевых правил противостояния обману (методам социальной инженерии)

ПОМОЩЬ ДЛЯ ПОДБОРА АРГУМЕНТОВ:

Раскрыть подробнее предложенные аргументы/добавить свои:

Примеры уже имеющихся внедренных технологий и того, как они влияют на безопасность операций:

- NFC
- 3D Secure-код
- Менеджер паролей
- Биометрия как дополнительная защита для сочетания с традиционной
- VPN (частная сеть с шифрованием)
- Новые антивирусы и программы

Если не быть в тренде, то мошенники всегда будут опережать – пример со снятием денег в банкомате без карты по последним цифрам входящего звонка или по QR-коду

Статистика + примеры того, что социальная инженерия (т.е. психологическое манипулирование), а не технологии влияют больше на успехи мошенников

Непроверенные временем новейшие технологии могут быть рискованны.
Пример – биометрия (если утечка отпечатков пальцев, их не поменяешь, как пароль)
VPN и менеджеры паролей – зависит от доверия к провайдерам и разработчикам

Некоторые модные «фишки» могут необоснованно ослабить бдительность



ТЕЗИС

Согласия на обработку персональных данных, которые мы даем тем, кто оказывает нам услуги, повышают защиту этих данных

КОНТРЕЗИС

Согласия на обработку персональных данных, которые мы даем тем, кто оказывает нам услуги, не влияют на безопасность этих данных

ПОМОЩЬ ДЛЯ ПОДБОРА АРГУМЕНТОВ:

Раскрыть подробнее предложенные аргументы/добавить свои:

Согласия дают новые возможности для получения услуг удаленно (пример – цифровой профиль гражданина и др.), а значит сокращают цепочки посредников и снижают риски

Если с вас берут при оказании услуг согласие, то значит соблюдается закон о персональных данных (152-ФЗ), а следовательно и правила их обработки и хранения. Значит согласия – дополнительная гарантия безопасности.

Согласие позволяет ограничить того, кто использует твои данные (пример с согласием на распространение ПНд – какие категории данных можно разрешить сайту о себе печатать с отзывом, а какие нет)

Выдавая согласия, ты не можешь повлиять на риски утечек их из баз данных компаний, которые их обрабатывают (статистика роста утечек ПДн и громкие примеры утечек)

Большинство относятся к подписанию согласий безответственно – особенно, если они выдаются в электронном виде (галочка на сайтах). Не осознают что, зачем и на какой срок выдают. Есть риск, что передаешь больше чем нужно для услуг на каком-то сайте. Значит сами по себе согласия не повышают безопасность, если не умеешь ими правильно управлять

ТЕМА 3. Осторожно, финансовые пирамиды!



ФИНАНСОВАЯ
БЕЗОПАСНОСТЬ
В ЦИФРОВОМ МИРЕ

ТЕЗИС

Финансовые пирамиды прошлого опаснее, чем пирамиды XXI века

КОНТРЕЗИС

Финансовые пирамиды XXI века опаснее, чем пирамиды прошлого

ПОМОЩЬ ДЛЯ ПОДБОРА АРГУМЕНТОВ:

Раскрыть подробнее предложенные аргументы/добавить свои:

Финансовые пирамиды прошлого имели колоссальный охват и число жертв (примеры, MMM, Властелина).
Сейчас не те масштабы

Раньше люди были более доверчивы, т.к. не было возможности провести полноценный фактчекинг (проверку информации о пирамиде в интернете, так как он еще не был так распространен), в то время как на телевидении шла только позитивная реклама (пример массовой доверчивости – митинги в поддержку арестованного Мавроди)

Сейчас больше защиты со стороны государства – ужесточение наказания (специальные статьи закона), организации, помогающие жертвам пирамид, фонд, в котором можно получить компенсацию.

Сейчас у пирамид намного больше способов маскировки – они нацелены не на массовую аудиторию, а на разные целевые группы – пенсионеров, подростков, студентов, желающих инвестировать в крипто-активы. Поэтому легче стать жертвой сейчас (примеры маскировки – под онлайн-игры для подростков, под крипто-проекты – Финико, Кэшбери, под сельскохозяйственные кооперативы для пенсионеров).

Сейчас стерлись границы, так как пирамиды перешли в сеть – создатели пирамид могут находиться в другой стране (например – создатели мошеннических онлайн-игр «Веселые рыбаки»), а значит их сложно найти и вернуть свои деньги.

Современные пирамиды могут серьезно отличаться сроком жизни от пирамид прошлого (менее месяца), закрываются одни и открываются другие, жертве очень сложно сориентироваться и вывести деньги вовремя



ТЕЗИС

При создании и хранении надежного пароля лучше рассчитывать на себя, чем на помощь различных сервисов по проверке, генерации и хранению

КОНТРЕЗИС

При создании и хранении надежного пароля лучше использовать различные сервисы по проверке, генерации и их хранению, чем рассчитывать на себя

ПОМОЩЬ ДЛЯ ПОДБОРА АРГУМЕНТОВ:

Раскрыть подробнее предложенные аргументы/добавить свои:

Сложный пароль можно создать и самому, если использовать специальные техники запоминания (мнемотехники), когда берешь понятное тебе слово и усложняешь его – перемешиваешь с цифрами и символами (пример). А еще соблюдать главные требования к длине и другим характеристикам. А у менеджеров паролей разные рейтинги надежности, вдруг выберешь не тот. Кроме того, надо знать, где они хранят пароли – на сервере или на твоих же устройствах, которые могут сломаться или потеряться.

Когда пользуешься сервисом по проверке паролей, надо ему доверять – а вдруг твой пароль потом используют.

Хранить пароли можно даже дома в тетрадке, если сложно запомнить, главное – не на самих устройствах

Менеджеры паролей – программы-сейфы с очень надежным шифрованием. Некоторые помогают сгенерировать сложный пароль. Просто надо ответственно подойти к выбору программы и узнать рейтинги. Такой сложный пароль придумать и главное запомнить человеку сложно, а тетрадка, в которую записал может потеряться или стать доступна другим.

Чтобы проверить пароль можно использовать сервисы по проверке его надежности, но если не очень доверяешь – проверь сложность конструкции пароля, а потом немного измени его.

Даже пароль от аккаунта от твоей электронной почты – может быть программой хранения других паролей. Использовать такую опцию этого сервиса – дополнительное удобство для современного человека