Какие базовые темы нужно раскрыть в обучающих материалах для повышения осведомленности сотрудников

Другач Юрий

Участник Bug Bounty Яндекс, Google, PayPal

Автор статей в журнале «Хакер»

Веду блог о соц. инженерии: icast.ru

Видео deepfake

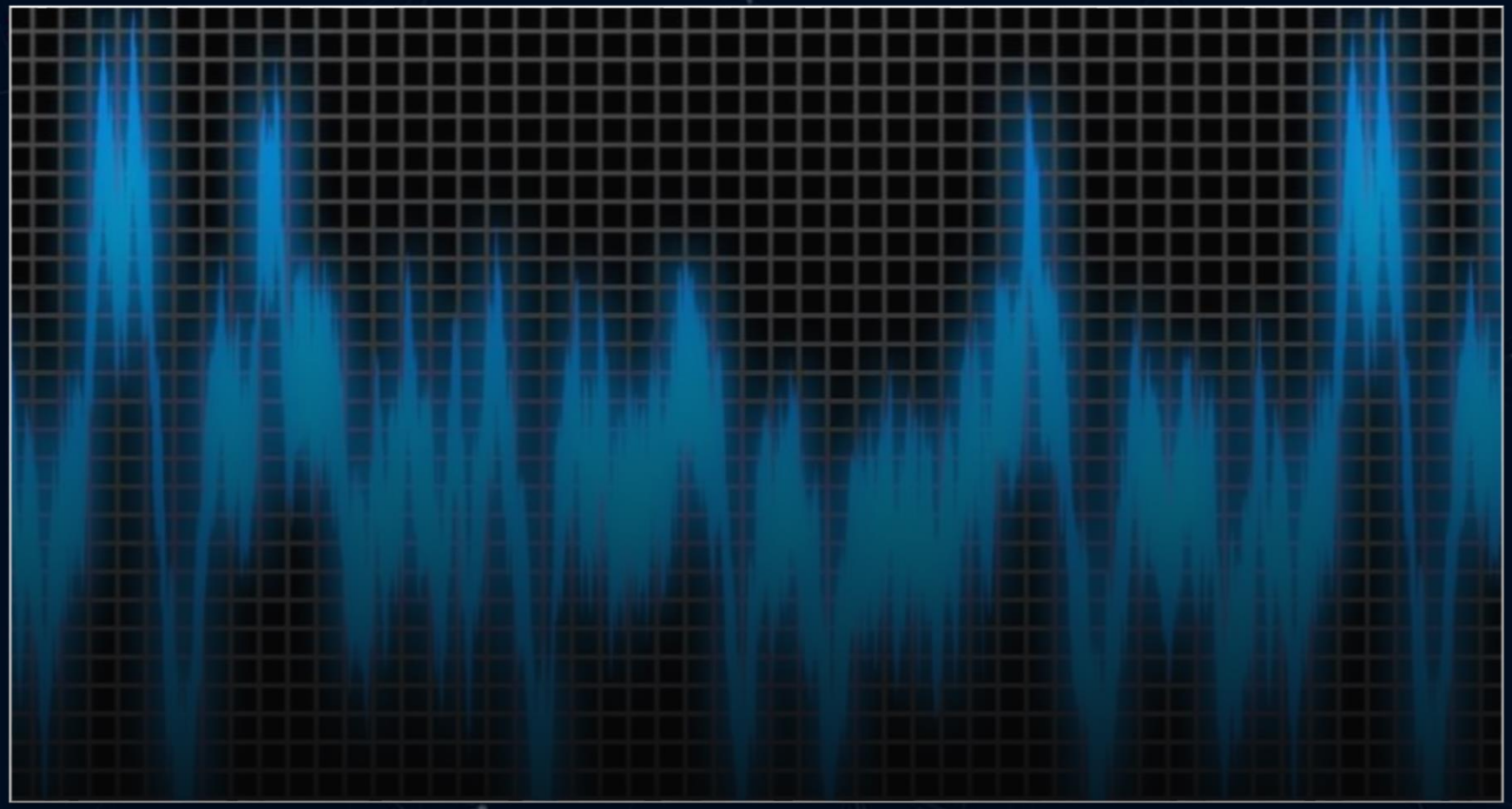
Дезинформация, снижение лояльности сотрудников, вымогательство/шантаж, требование выкупа

Сценарии атак «Find trap»

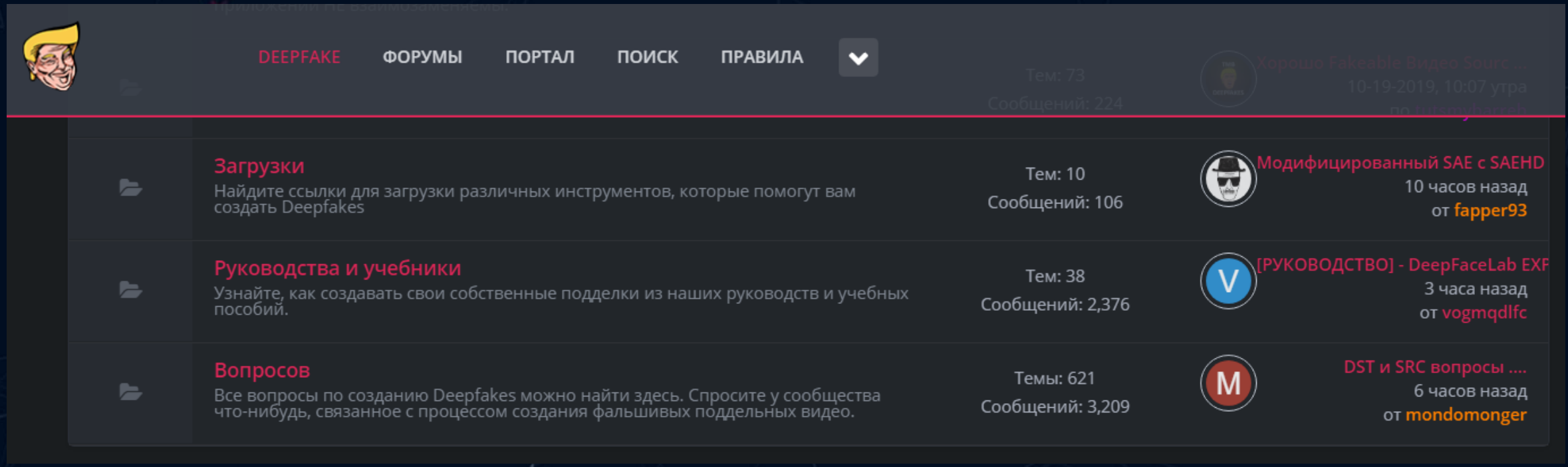
или самостоятельный поиск ловушки

Голосовой deepfake

- 220 000 €



Кто первый


DEEPFAKE
ФОРУМЫ
ПОРТАЛ
ПОИСК
ПРАВИЛА
Загрузки
Найдите ссылки для загрузки различных инструментов, которые помогут вам создать Deepfakes
Тем: 10
Сообщений: 106
Модифицированный SAE с SAEHD
10 часов назад
от fapper93
Руководства и учебники
Узнайте, как создавать свои собственные подделки из наших руководств и учебных пособий.
Тем: 38
Сообщений: 2,376
[РУКОВОДСТВО] - DeepFaceLab EXF
3 часа назад
от vogmqdlfc
Вопросов
Все вопросы по созданию Deepfakes можно найти здесь. Спросите у сообщества что-нибудь, связанное с процессом создания фальшивых поддельных видео.
Темы: 621
Сообщений: 3,209
DST и SRC вопросы ....
6 часов назад
от mondomonger

Базовое обучение

- Как хакер может испортить жизнь лично вам.

- В офисе или возле него найдено устройство с USB, что делать.

- Как распознать вредоносную ссылку (10 признаков).

- Как распознать вредоносное вложение в письме (без архивные и архивные вложения, .html вложение).

Базовое обучение

- Как хакеры входят в доверие (многоходовые атаки, векторы атак с использованием СИ).

- Проверяем отправителя (включая вариант, когда легитимного отправителя взломали).

- Определяем хакерское письмо по тексту.

- 4 вредоносных сценария, которые используют хакеры в письме (файлы, ссылки, фишинг, выманивание информации).

Персонализированное обучение

В зависимости от браузера:

- Установка дополнений в браузере.

- Сохранение пароля в браузере.

Персонализированное обучение

В зависимости от внутренних правил:

- Какие данные нельзя отправлять по email.

- Действия при обнаружении взлома email.

- Что делать, если вы сомневаетесь, кто вам пишет. (уточнить/найти доп. информацию, проигнорировать, переслать в СБ)

- Какие сообщения стоит игнорировать, а о каких сообщать в СБ? (много повторяющихся бесполезных рапортов – создаем правило и делаем известным).

- Как проверить файл в 50 антивирусах.

- Как безопасно открыть и проверить ссылку.

Персонализированное обучение

В зависимости от парольной политики:

- Создание надежного и простого для запоминания пароля.

- Безопасное хранение пароля.

- Кому можно сообщать свои пароли.

- Использование одинаковых паролей на разных ресурсах.

Персонализированное обучение

В зависимости от взаимодействия подразделений:

- Что делать, если из одного отдела пришло подозрительное письмо в другой отдел.

Памятка по информационной безопасности

На Хабре: https://habr.com/ru/post/486176/

В блоге: https://icast.ru/?p=362

Спасибо за внимание!

Другач Юрий: fb.com/yuresd

Email: dys@icast.ru

Блог о социальной инженерии: icast.ru