Защита инфраструктуры: разглядеть леопарда за пятнами.

Понять реальный объём. Обучить работников кибергигиене своими силами, увернуться от фишинга.

Знание только тогда знание, когда оно приобретено усилиями своей мысли, а не памятью.

(С) Лев Толстой

Куличкин Артём Александрович

CISM, CISA, CEH, CND.

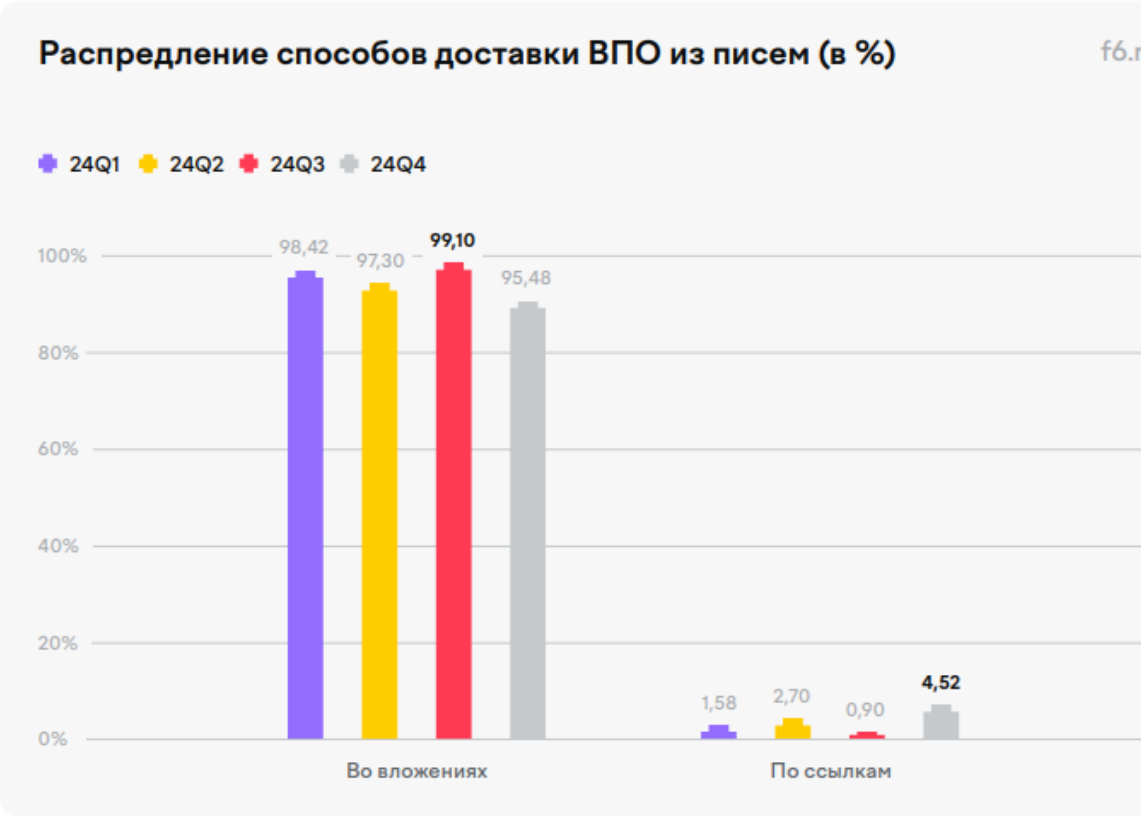
И. о. Директора по информационной безопасности дочерних компаний, АО «СОГАЗ»

Актуальность

- Рост фишинга
- Рост мошенничества в мессенджерах
- Фишинг, мошенничество в мессенджерах
- Продажа RU credentials

- **Рост мошенничества в мессенджерах**, в частности, в Telegram. Данный мессенджер предоставляет множество способов размещения мошеннического и фишингового контента: публичные каналы, публичные чаты, Telegram-боты.
- **В 2024 году** среднее количество создаваемых **фишинговых сайтов** на один бренд **увеличилось на 52%** по сравнению с 2023 годом, среднее количество создаваемых **мошеннических ресурсов** на один бренд **увеличилось на 17%**.
- Несмотря на мнение, что на даркнет-форумах существует запрет для работы против России и СНГ, мы находили объявления о продаже доступов в компании в этих регионах. В 2024 году мы обнаружили в продаже **9 корпоративных доступов** стран СНГ.
- В 2024 году не менее **17** группировок **хактивистов** атаковали российские и белорусские организации. Годом ранее таких групп было как минимум **13**.

Актуальность



Актуальность

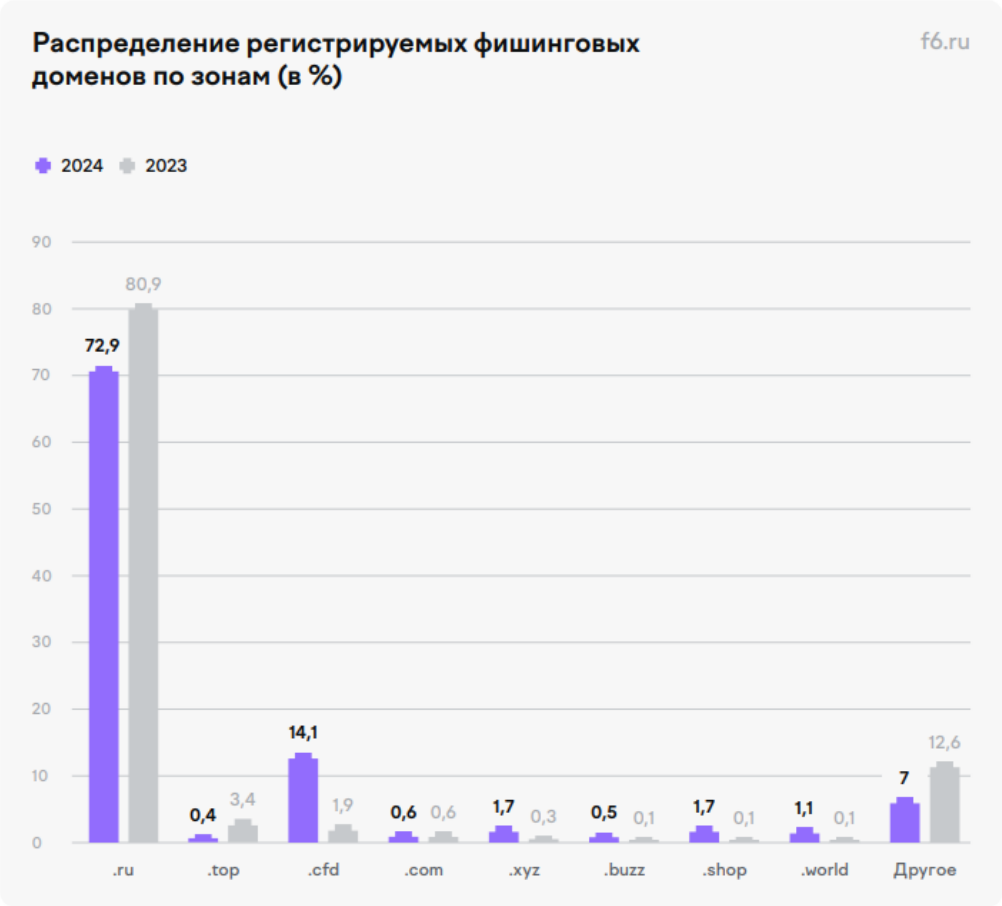


Рисунок 9. Украденные данные (доля успешных атак на организации)

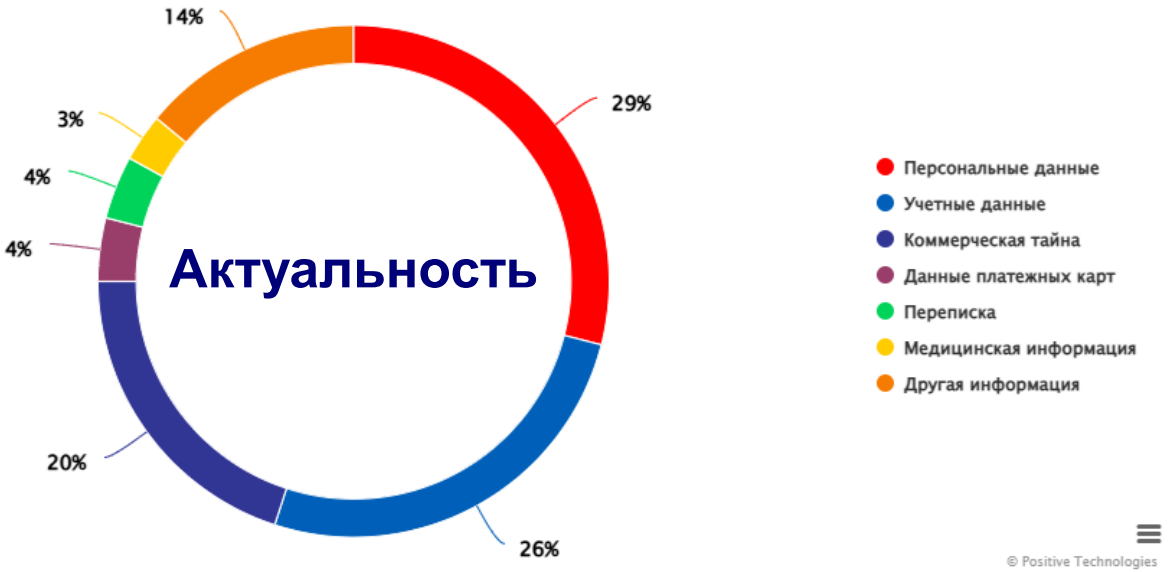


Рисунок 14. Методы атак (доля успешных атак)

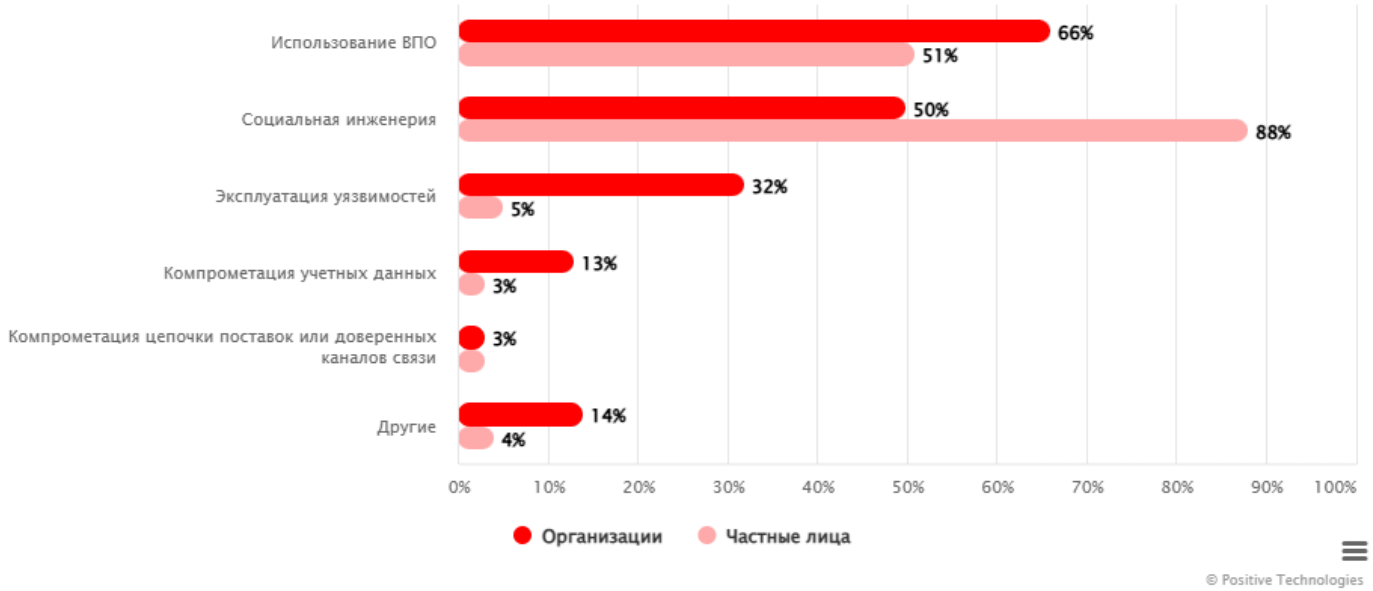
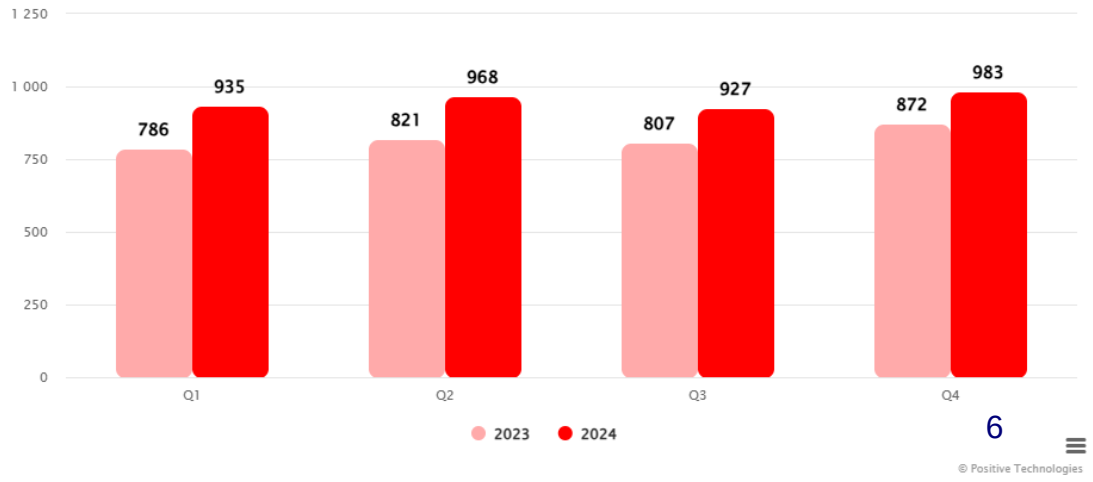
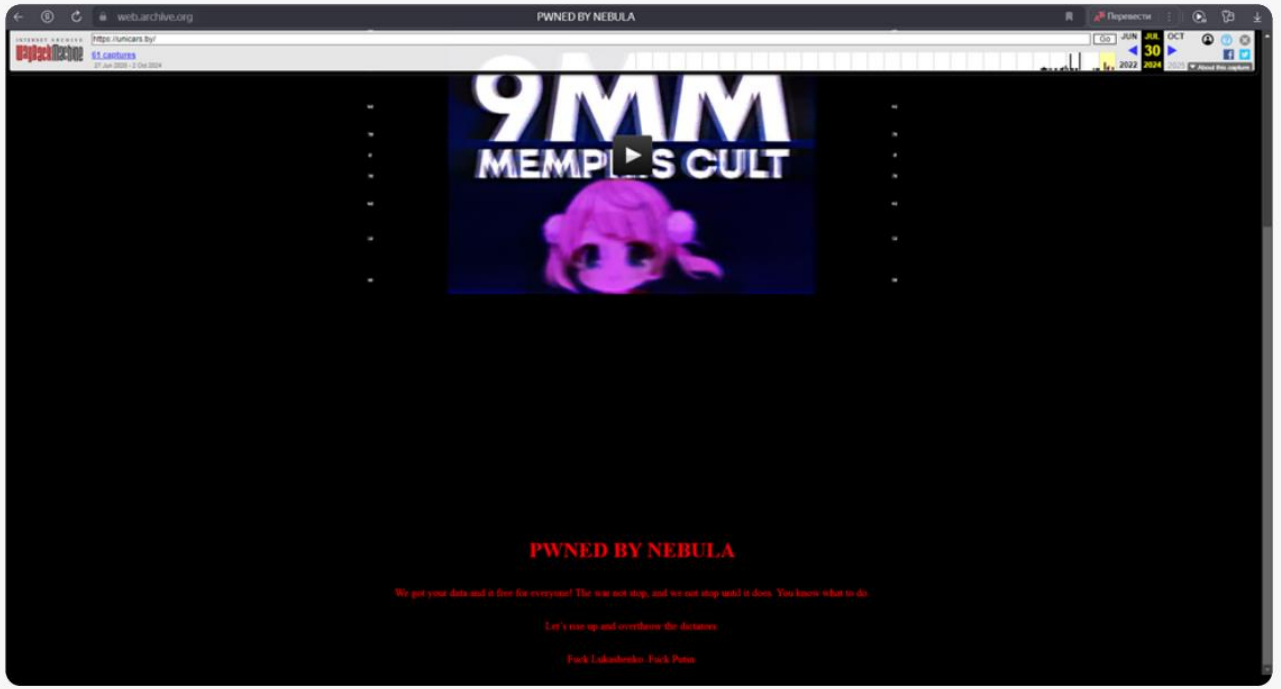


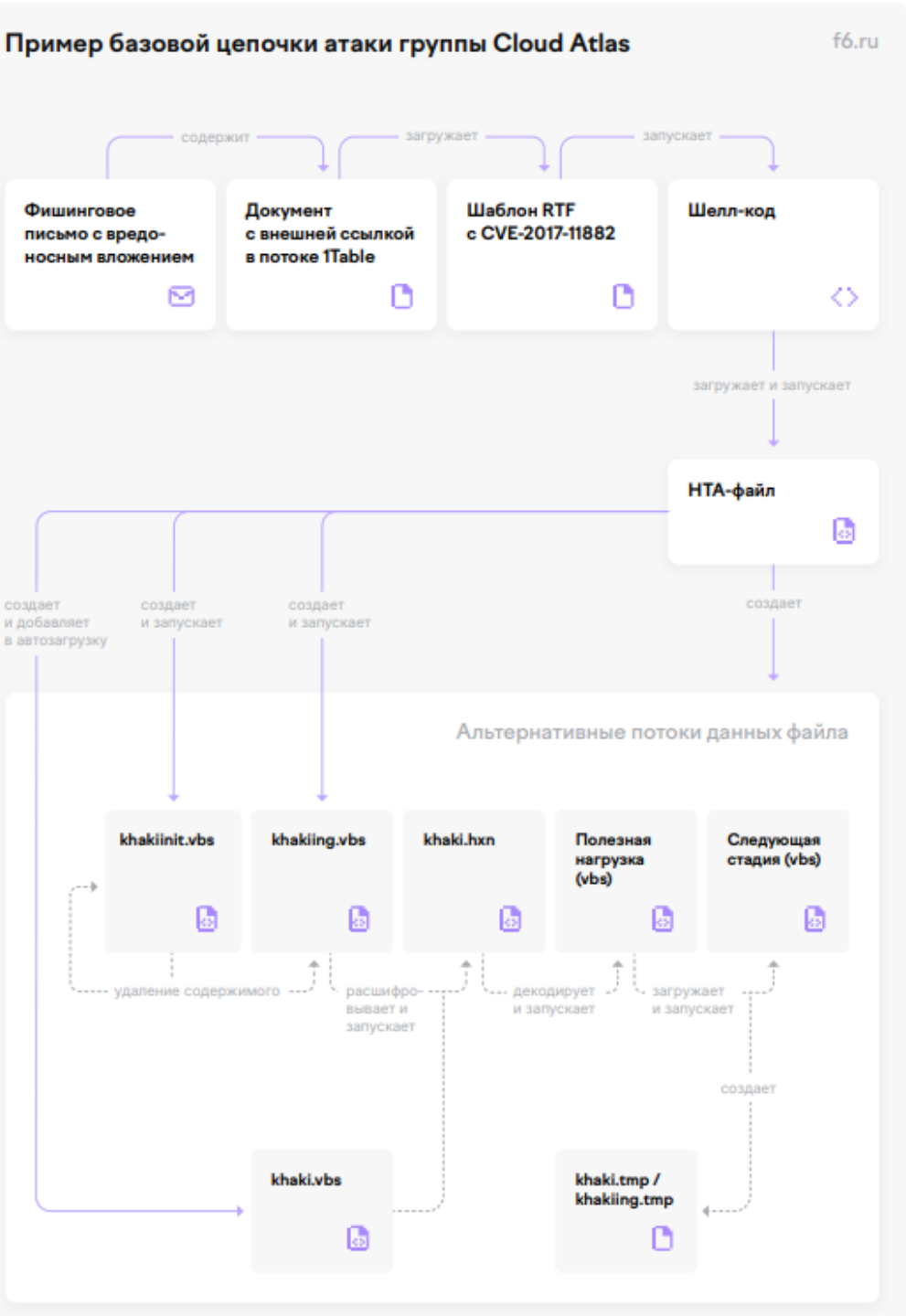
Рисунок 11. Количество инцидентов в 2023 и 2024 годах (по кварталам)



Как атакуют?

Пример Атаки одной из группировок





План

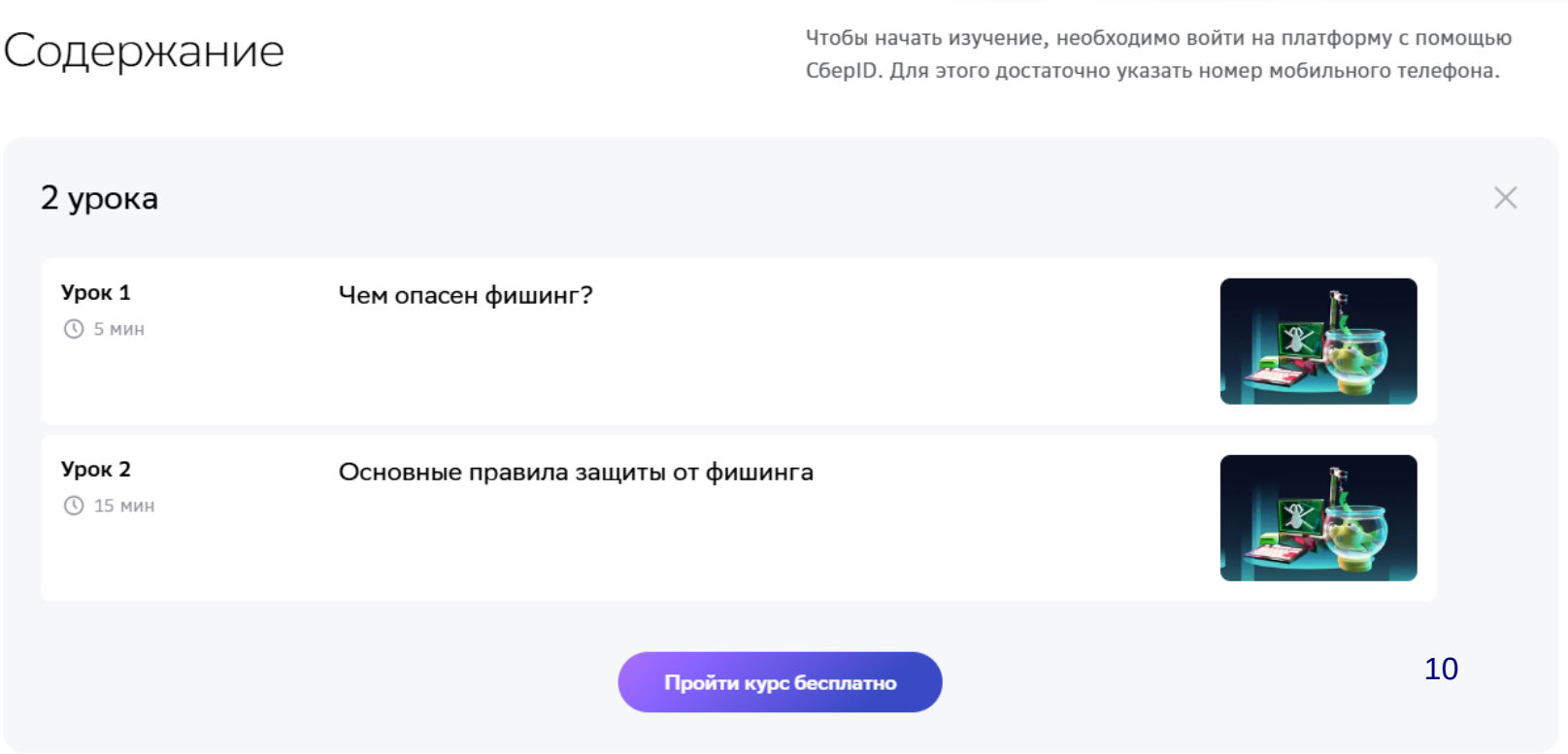
1. Разработать обучение для работников
2. Купить домен
3. Подготовить инфру
4. Развернуть Gophish
5. Собрать список работников у кадров
6. Разработать сценарии фишинга
7. Оценить каждого работника после
8. Метрики обучающего фишинга
9. Оценить общую реакцию на учебный фишинг
10. Отправить на новое обучение

План

1. Разработать обучение для работников
2. Купить домен
3. Подготовить инфру
4. Развернуть Gophish
5. Собрать список работников у кадров
6. **Разработать сценарии фишинга**
7. Оценить каждого работника после
8. Метрики обучающего фишинга
9. Оценить общую реакцию на учебный фишинг
10. Отправить на новое обучение

Разработать обучение для работников

- Посмотреть, как это делают другие
- Специализируем обучение под вашу компанию
- Обращаем внимание на мелочи
- Тест с живыми примерами и игровой форме



Купить домен

Выбираем домен используя ИИ

Генератор доменных имен на основе ИИ

Используйте возможности искусственного интеллекта для поиска новых и креативных идей для доменных имен.

Придумай различное написание слова Kolbasa изменяя буквы внутри слова, что бы человек не заметил разницы, используй различные доменные зоны com ru su и другие

Расширенные настройки

Генерировать домены

У вашего доменного имени другой регистр? Перенести сегодня

Kolbasa.ru

K0lbasa.ru

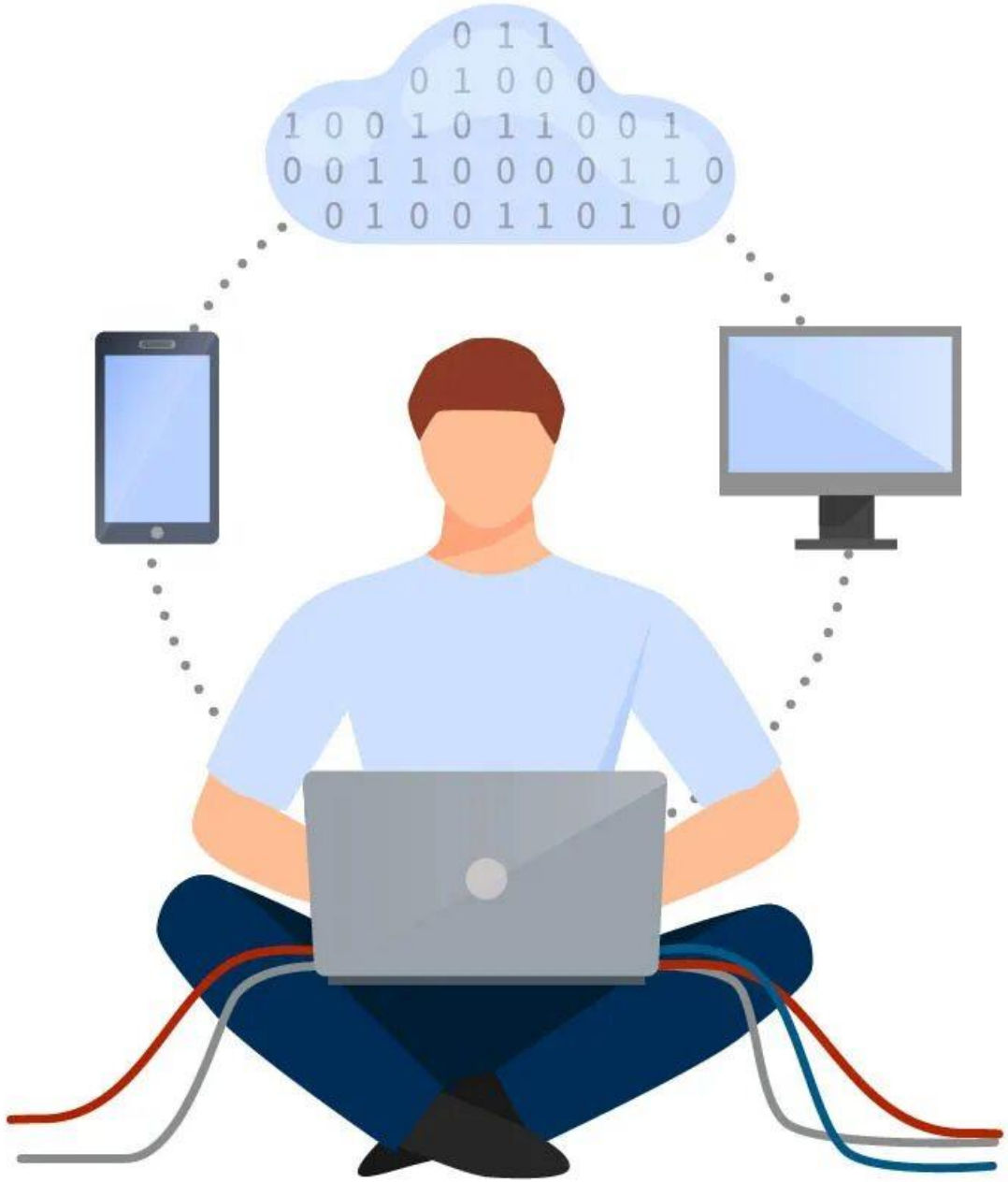
Kolbasa.ru.com

Kolbaza.ru

Kolba.su

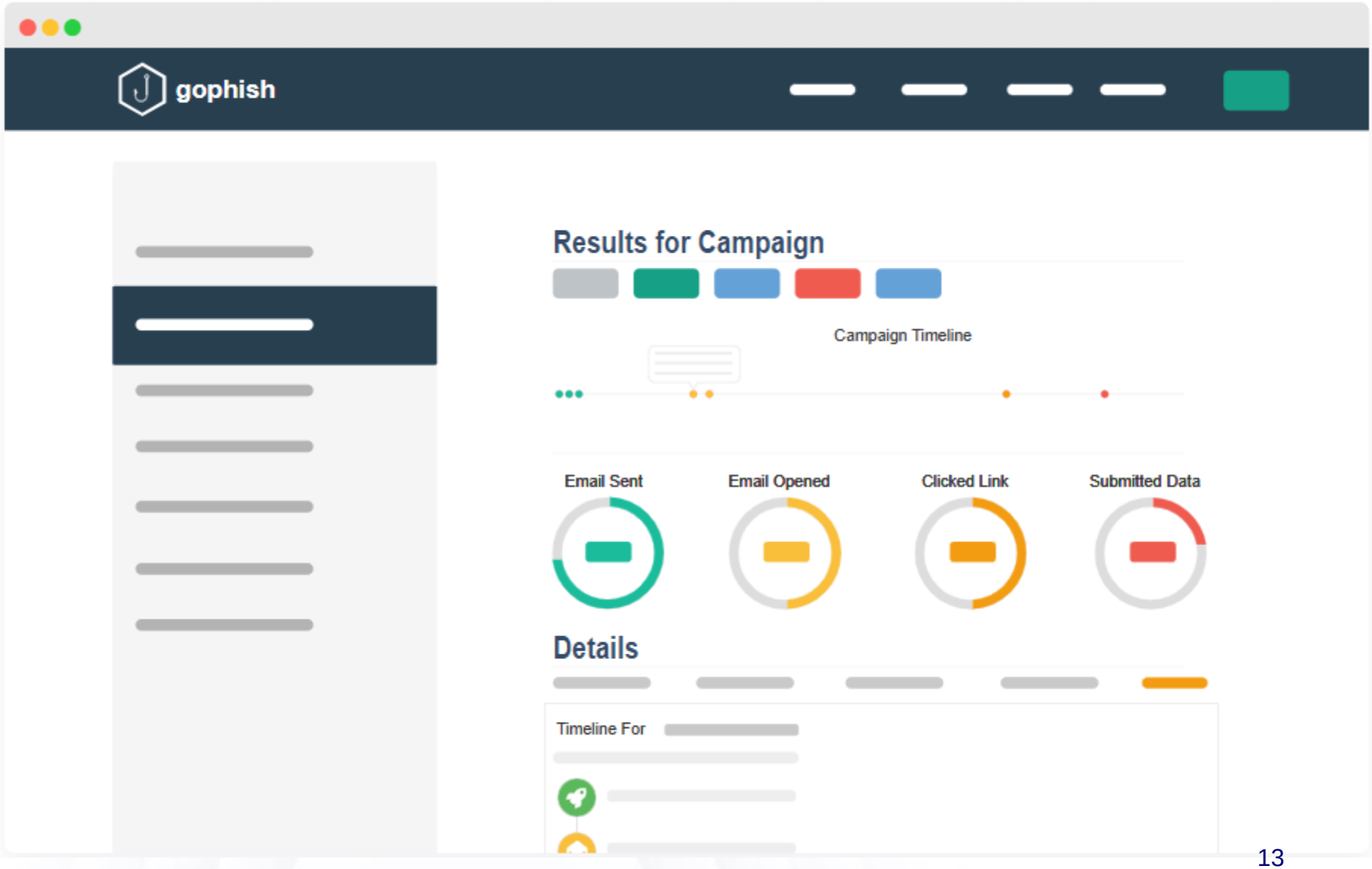
Подготовить инфру

1. Публикуем (доступно извне)
2. Настраиваем сервис безопасно (обновляем, отключаем админку, access list и др.)



Развернуть и настроить Gophish

1. [Gophish - Open Source Phishing Framework]



Собрать список работников у кадров (не из AD)

Собираем список работников

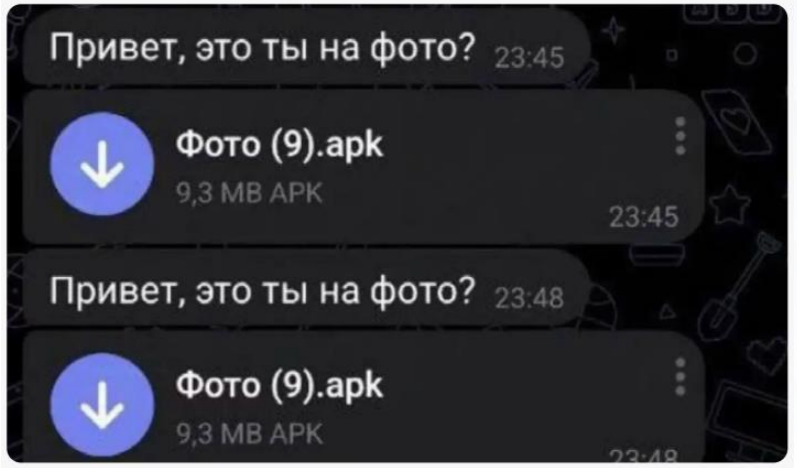
1. Разбиваем на категории: финансисты, IT, ТОПы, юристы, АХО и тд.
2. А также общий список

Разработать сценарии фишинга (лёгкий, средний, сложный)

1. Первая рассылка после обучения (стартовая точка)
2. Сценарии для узких категорий работников
3. Общая рассылка третированная под вашу компанию (разбитая по времени)
4. Таргетированная рассылка с использованием данных соц. сетей*

Примеры:

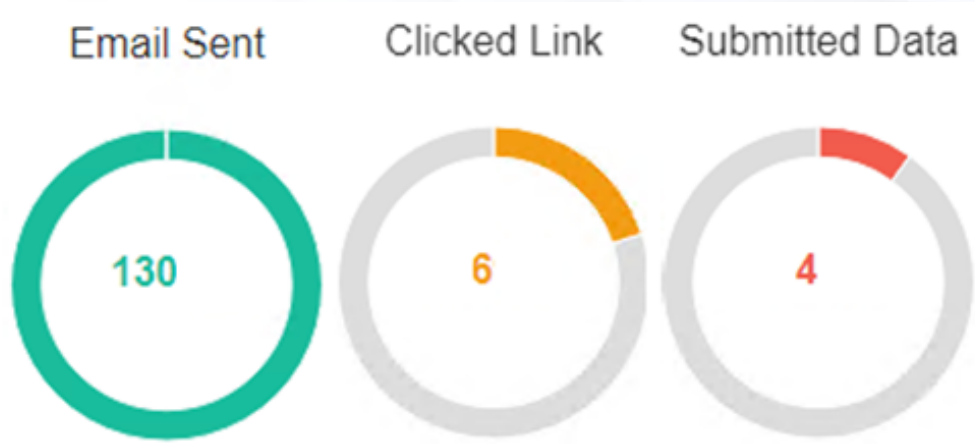
1. Штраф из «Госуслуг»
2. Выигрыш билетов на спектакль
3. Ваш пароль попал в список скомпрометированных
4. Срок действия пароля истёк
5. Подарки от партнёров
6. Снимаем фильм про компанию
7. Фото с корпоратива
8. Изменения режима работы
9. Список под сокращение
10. Расчётный листок (чужая фамилия)
11. QR
12. CAPTCHA (PowerShell)



Оценить каждого работника

— выдержал атаку: +3
— открыл письмо: -1
— перешёл по ссылке: -2
— ввёл данные в форму: -3

ИТОГ:



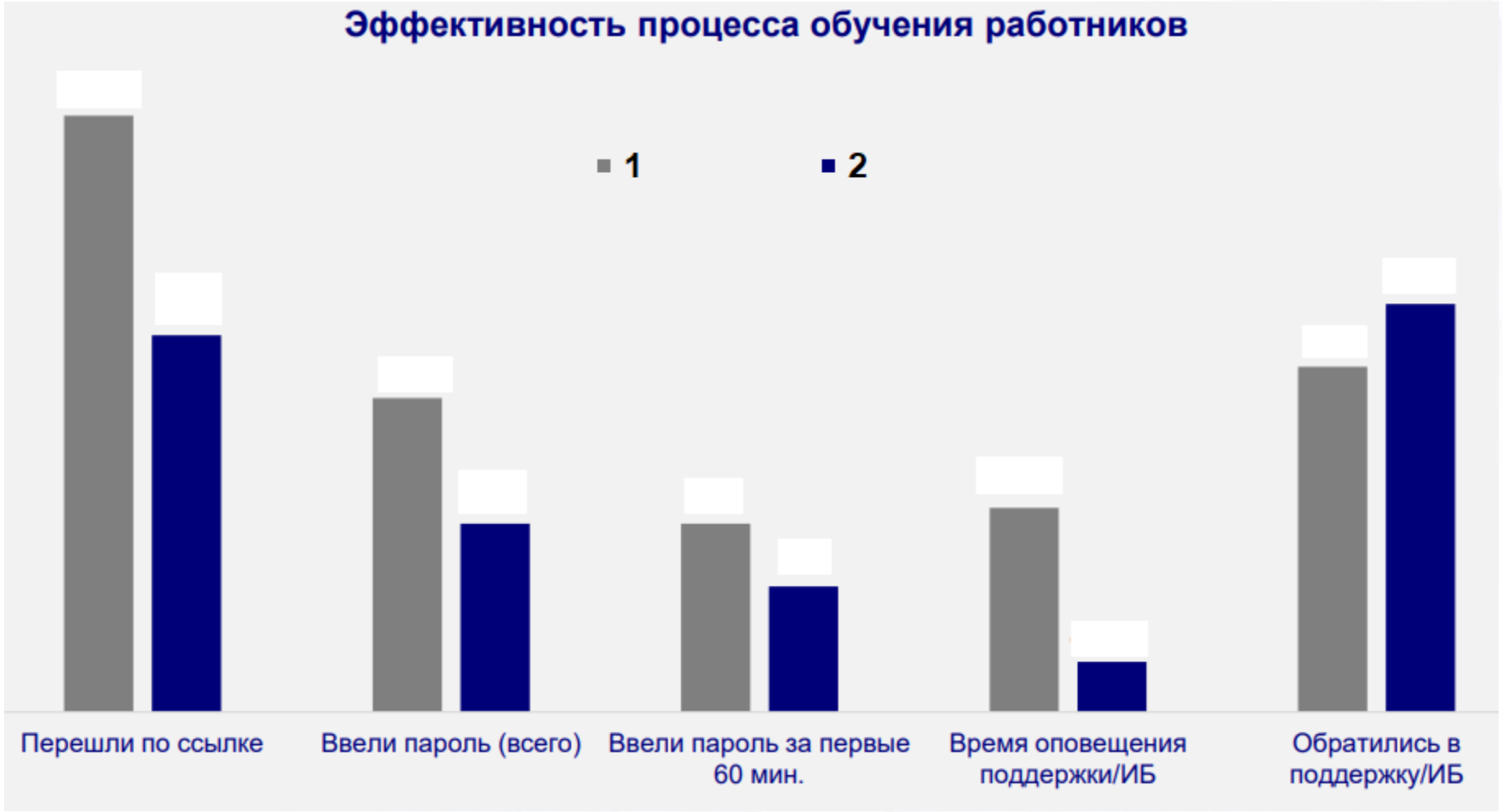
	Name	Created Date				
3	**Оценка качества обслуживания.**	November pm	, 12:48:16	4	6	1
2	**Налоговый вычет.**	November pm	, 12:47:24	4	1	6
1	**Копилка онлайн.**	November pm	, 12:45:36	4	9	5

Метрики обучающего фишинга

- Количество прошедших обучение
- Процент открытия писем
- Процент кликов по ссылкам
- Процент ввода учётных данных
- Процент сообщивших о фишинге
- Время первого сообщения о фишинге
- Количество повторных кликов по ссылке
- Количество пересланных сообщений
- Количество самостоятельной смены пароля

Сравниваем с предыдущими кампаниями

Оценить общую реакцию на учебный фишинг



Отправить на новое обучение

Кто попался на повторное обучение
Кто был внимателен на более сложное обучение
Кто регулярно не попадается использовать новые методы (обратная соц. Инженерия, USB и тд.)

ВЫ БЫЛИ НЕ ВНИМАТЕЛЬНЫ И ПЕРЕШЛИ ПО ФИШИНГОВОЙ ССЫЛКЕ.

Как защититься от фишинга: 10 советов
Иногда киберпреступники отправляются на рыбалку. ТолькС их золотая рыбка — это ваши данные. Итак, что нужно сделать, чтобы защитить себя от фишинга?
Даже если слово «фишинг» ассоциируется у вас исключительно с рыбалкой, вы не так уж далеки от истины. Только в роли «рыбаков» в Интернете выступают мошенники, а в роли «рыбки» — чужие персональные данные, логины и пароли к финансовым аккаунтам добропорядочных пользователей и так далее.
От фишинга нет универсального лекарства, кроме бдительности нТ грани паранойи. Проблема в том, что эта зараза похожа на грипп — постоянно мутирует и меняет методы атак_. Мошенники, стоящие за фишинговыми операциями, могут запустить персональную кампанию, направленную, например, только на сотрудников оп]еделенной организации или лишь на кормящих матерей. Такой вредоносный маркетинг. Способов попасться масса: подключиться к публичному Wi-Fi в кафе с авторизацией по учетной записи социальной сети, ввести свои данные на поддельном сайте, перейти по ссылке в очередном письме счастья на Новый год или черную пятницу… Всего не перечислишь.

В общем, заполучить эту проблему легко. А как себя защитить?

1. ВсегПа внимательно проверяйте ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта. Если с написанием что-то не так, это верный признак, что мошенники подсовывают вам поддельную страницу.

2. Перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где «s» означает secure — безопасное), то все в порядке.

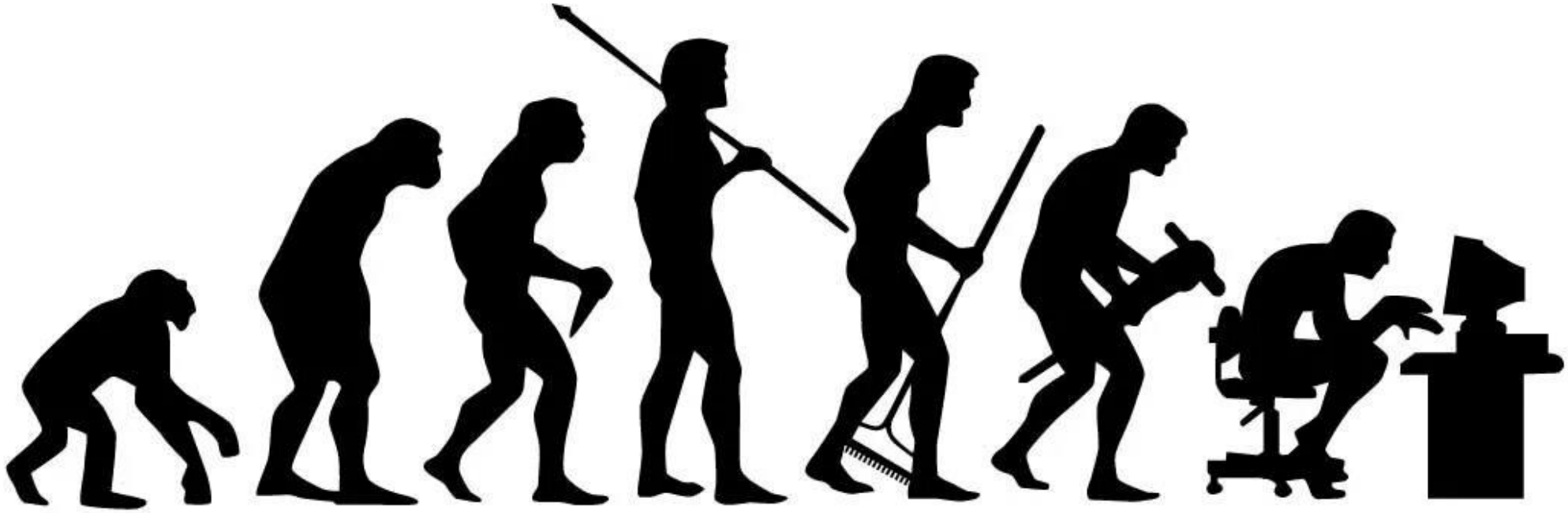
3. Даже если письмо ↑ли сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.

4. То же самое касается писем, отправленных из официальных инстанций и организаций: банков, налоговой, онлайн-магазинов, бюро путешествий, авиакомпаний и так далее. Даже с вашей работы. Не так уж трудно подделать официальное письмо настолько достоверно, что от реального его отличить будет очень сложно.

5. Иногда фальшивые письма и фальшивые сайты 3о всем повторяют дизайн настоящих. Качество подделки зависит от того, насколько хорошо преступники выполнили «домашнюю работу». А вот гиперссылки, скорее всего, будут неправильные — или с ошибками, или вообще будут ссылаться не туда. По этим признакам можно отличить фишинговое письмо от настоящего.

Заключение

Развивайте критическое мышление работников и превращайте в знания усилиями своей мысли, а не памятью.



Спасибо
за внимание