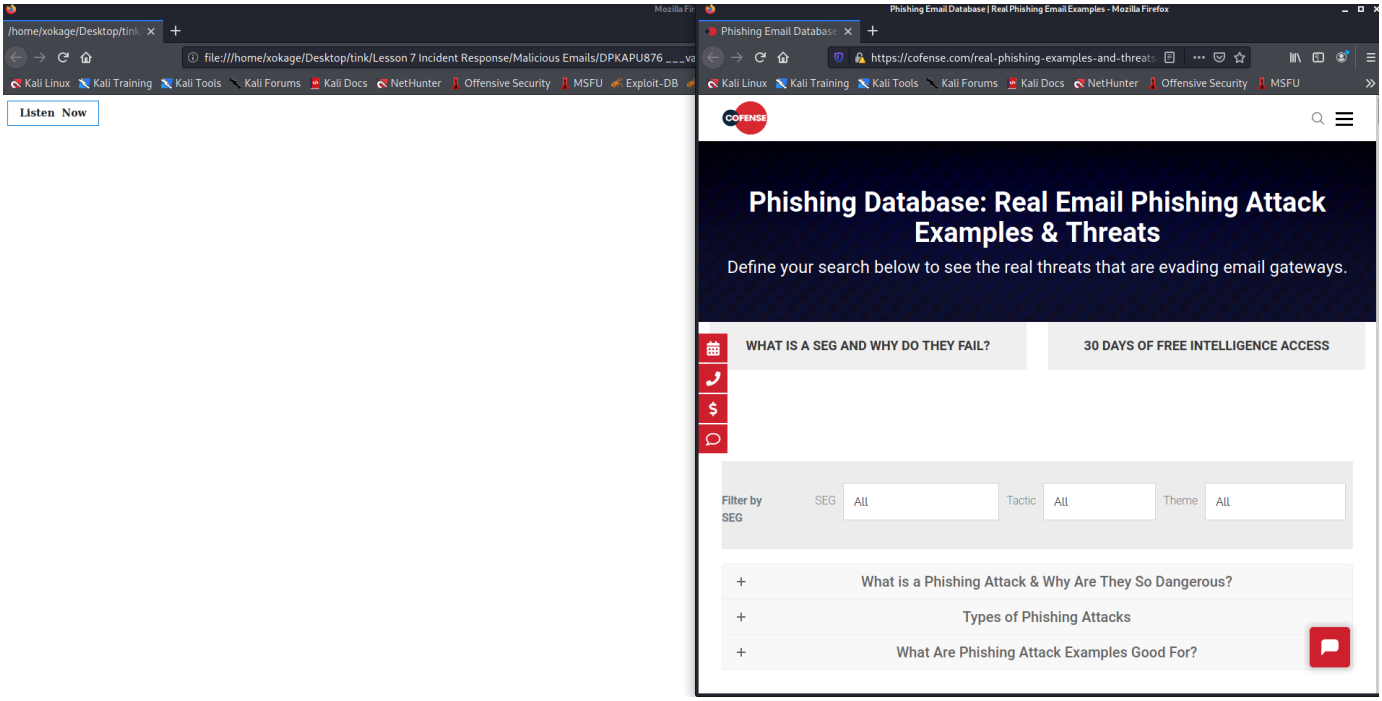
Homework - [Lecture 7] - Incident Response

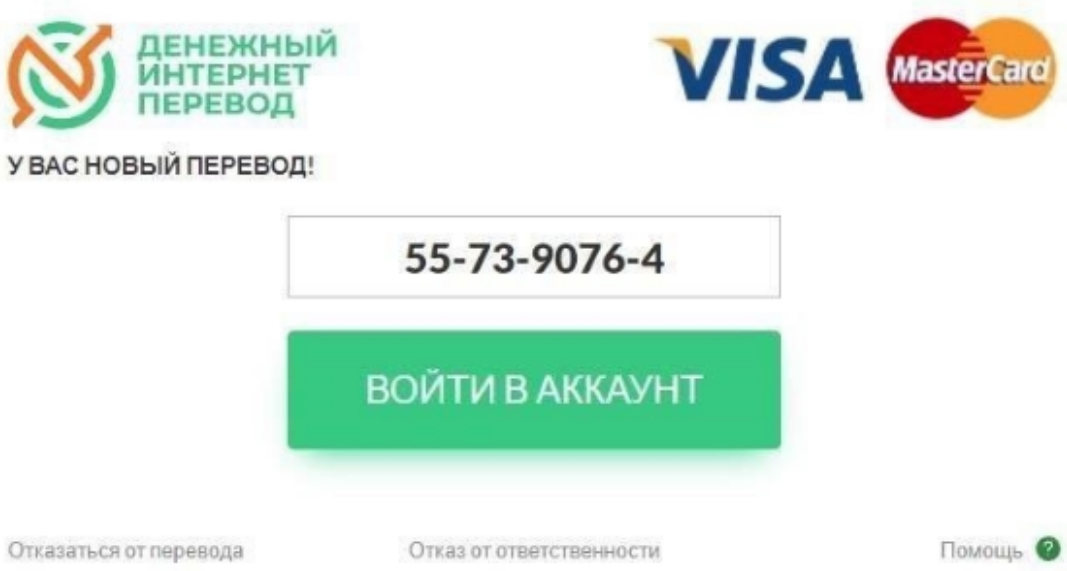
Задание 1

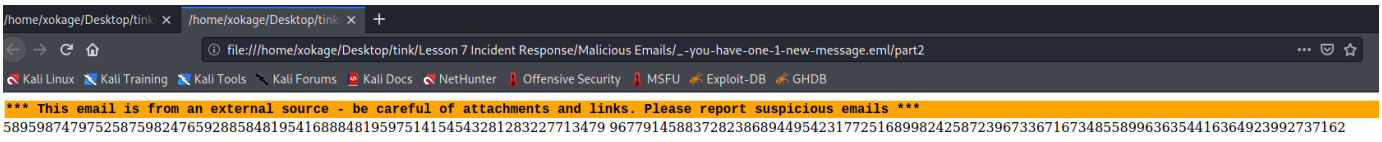
У нас есть два письмаЮ будем называть их так:
Первое письмо - DPKAPU876;

```
From: Microsoft Office <help@microsoft.com>
To: "jchancey" <jchancey@augusta.edu>
Subject: Voicemail received for you
x-originating-ip: [67.134.174.58]
Content-Type: multipart/related;
        boundary="_001_MW3PR19MB10294734C40E2B82FADBB1E3B2210MW3PR19MB4876namp_";
        type="multipart/alternative"
MIME-Version: 1.0
Return-Path: <account123@scammail.net>


--_001_MW3PR19MB10294734C40E2B82FADBB1E3B2210MW3PR19MB4876namp_
Content-Type: multipart/alternative;
        boundary="_002_MW3PR19MB10294734C40E2B82FADBB1E3B2210MW3PR19MB4876namp_"

--_002_MW3PR19MB10294734C40E2B82FADBB1E3B2210MW3PR19MB4876namp_
Content-Type: text/plain; charset="us-ascii"




--_002_MW3PR19MB10294734C40E2B82FADBB1E3B2210MW3PR19MB4876namp_
Content-Type: text/html; charset="us-ascii"

<div style="text-align: left;">
        <a class="x_secondaryButton x_font" role="button" style="margin: 0px; padding: 6px 16px 7px; border: 1px solid rgb(0, 120, 212); border-image: none; text-align: center; color: rgb(33, 33, 33); line-height: 20px; overflow: hidden; f
</div>
```



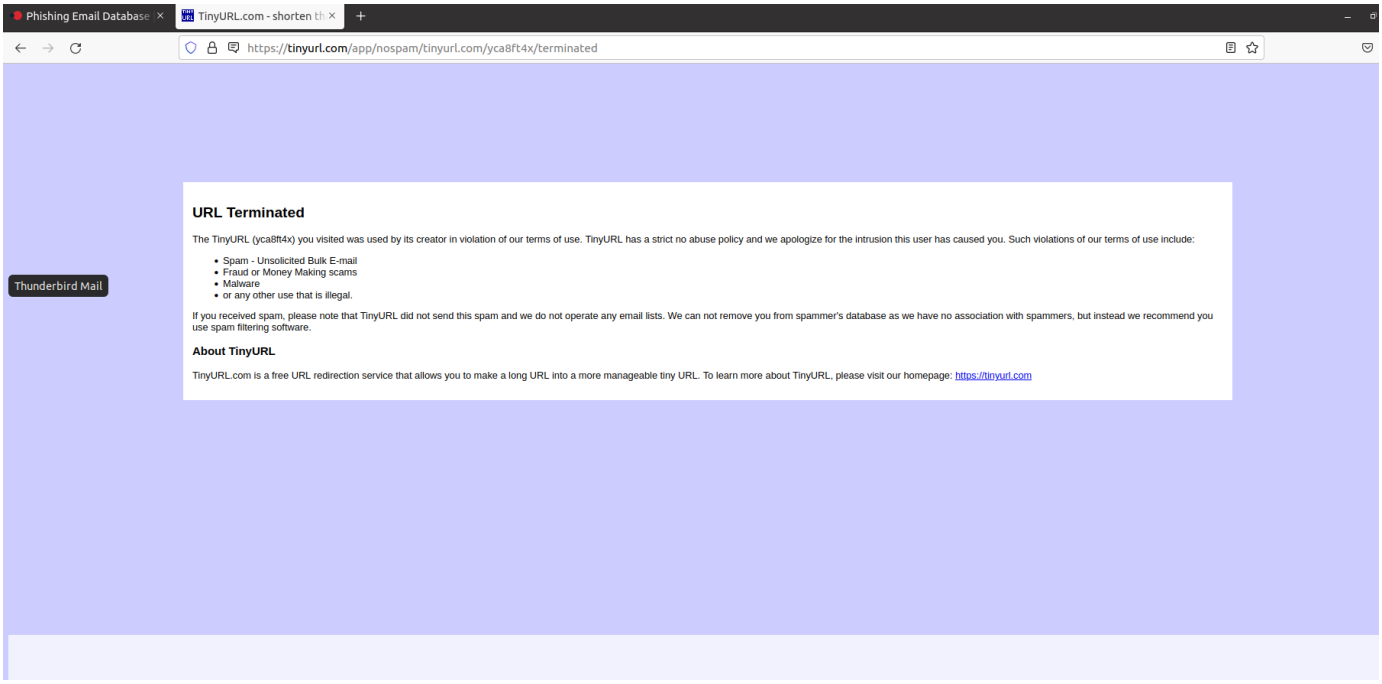
Второе письмо - you-have-one-1-new-message;





1. От кого эти письма?
   Ответ: Первое письмо от Microsoft Office help@microsoft.com (mailto:help@microsoft.com)
   Второе от Keiki
   5dehx55xep2wvzj2mm1h1o2q1bfpm4gejgn9q9ptgnbgmr1eaklusbhmi452st91q4k26eh5b4mshbd3rtkyg@edjcp8.ex-news.ru
   (mailto:5dehx55xep2wvzj2mm1h1o2q1bfpm4gejgn9q9ptgnbgmr1eaklusbhmi452st91q4k26eh5b4mshbd3rtkyg@edjcp8.ex-news.ru)
2. На какой почтовый ящик будет отправлен ответ на эти письма?
   Ответ: Первое письмо будет отправлено на почту Microsoft Office help@microsoft.com (mailto:help@microsoft.com)
   Второе на Keiki
   5dehx55xep2wvzj2mm1h1o2q1bfpm4gejgn9q9ptgnbgmr1eaklusbhmi452st91q4k26eh5b4mshbd3rtkyg@edjcp8.ex-news.ru
   (mailto:5dehx55xep2wvzj2mm1h1o2q1bfpm4gejgn9q9ptgnbgmr1eaklusbhmi452st91q4k26eh5b4mshbd3rtkyg@edjcp8.ex-news.ru)
3. Куда ведут ссылки? Что на этих ресурсах?

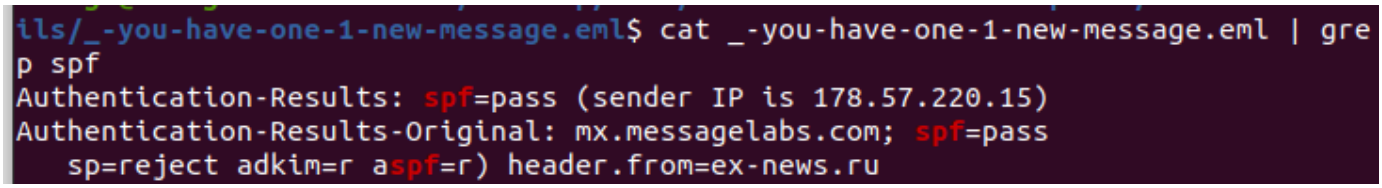
4. Что известно о доменах куда ведут ссылки?
   Ответ: Первое письмо ведет на https://cofense.com/real-phishing-examples-and-threats/ (https://cofense.com/real-phishing-examples-and-threats/)
   Это сайт компании cofense, которая занимается поставкой решений для защиты от зловреда в email письмах. На страничке примеры различных типов фишинга.
   Второе письмо ведет на https://tinyurl.com/yca8ft4x (https://tinyurl.com/yca8ft4x)



Сервис, что делает ссылки короче, видимо, заблочил редирект на ресурс.

5. md5sum - 7cdd69736af76a38c457af6f100f4344
   sha1sum - 686ee8e07a96bd8a2eb03b30171d9353baed1f6a

6. Прошли ли письма SPF? Какой вердикт?
   Ответ:
   У первого письма нет заголовка, второй прошел:



7. Было ли проверено вложение средством защиты? Какой вердикт?
   Ответ:
   Я понял, что не прошли, никакой информации по пройденным шагам без-ти нет

Задание 2

Имитируем ситуацию. Три часа ночи. Вы находитесь в ночной дежурной смене. Приходит алерт, что на Windows ноутбуке секретаря обнаружен подозрительный excel документ. Ноутбук находится в офисе.

1. Какие ваши первичные действия?
   Попробую дозвониться до работника
2. Что будете смотреть из логов, чтобы убедиться, что файл действительно вредоносный?
   В Журнале Событий поискать ивенты связанные с безопасностью. Посмотреть не закрепился ли малварь в шедулере.
3. Что будете делать с ноутбуком, с учетной записью? Каким образом?
   Учетную запись лучше блокнуть на время, через AD например.
4. Как будете доставать файл с ноутбука? Если вы используете инструменты, то опишите какие.
   Перекинуть файл на флешку и запускать на специальной VM с необходимыми инструментами для анализа.
5. Как файл мог оказаться на хосте? Опишите всевозможные варианты
   Секретарю отправили письмо, он открыл вложение, обычный excel документ, но в нем могут быть макросы, которые выполняются и закрепляются в системе;
6. Будете ли вы связываться с пользователем? Каким способом и почему?
   С пользователем я бы связался, чтобы выяснить как файл попал на рабочее ноутбук;
7. Не открывать письма, что приходят из неизвестных источников. Ставить антивирусы на рабочие машины