МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»

ИМКТ

Департамент информационной безопасности

Тананов Алексей Александрович
Жуков Владимир Владимирович

M9120-09.04.02ибкфс

ЛР № 2

«Проведение фишинговой атаки»

г. Владивосток

2022

Постановка задачи:

Провести 2 фишинговые атаки на почты gmail.com, mail.ru, dvfu.ru, protonmail.com со следующими критериями:

1. Первое письмо должно содержать документ с скриптом, отсылающий на сервер информацию о запущенной системе (canarytoken)

2. Второе письмо должно содержать ссылку, при переходе по которой пользователь

попадает на фишинговый сайт, содержащий копию формы авторизации. Форма авторизации берется на ваш выбор: двфу outlook, почтовый сервис mail, steam, Instagram, twitter.

3. Промежуток между отправкой писем должен составлять 24 часа и каждое письмо отсылается в 21:00 по UTC

4. Содержимое письма, заголовок и подпись должны максимально соответствовать выбранной тематики письма

Почты, используемые в лабораторной работе:

laoratornaadva1@protonmail.com: <pass>

laoratornaadva2@protonmail.com: <pass>

laoratornaadva3@protonmail.com: <pass>

laoratornaadva4@protonmail.com: <pass>

laoratornaadva5@protonmail.com: <pass>

laoratornaadva6@protonmail.com: <pass>

laoratornaadva1@gmail.com: <pass>

laoratornaadva2@gmail.com: <pass>

laoratornaadva3@gmail.com: <pass>

laoratornaadva4@gmail.com: <pass>

laoratornaadva5@gmail.com: <pass>

laoratornaadva1@mail.ru: <pass>

laoratornaadva2@mail.ru: <pass>

laoratornaadva3@mail.ru: <pass>

laoratornaadva4@mail.ru: <pass>

laoratornaadva5@mail.ru: <pass>

tananov.aa@dvfu.ru

zhukov.vvl@dvfu.ru

shapovalova.aal@students.dvfu.ru

gorbonos.nv@students.dvfu.ru

irgit.aa@students.dvfu.ru

Тематика писем:

Атака на отдел кадров. Письмо содержит информацию о изменении телефонов подразделений ДВФУ. Отсылается от имени одного из менеджеров ДВФУ.

Письмо 1:

Добрый день!
В связи со вступившими в силу изменениями внутренних номеров телефонов подразделений ШЭМ прошу ознакомиться с прикрепленным документом и принять сведения к работе.

С уважением,
Холодкова Наталья Васильевна

Главный менеджер
Административный отдел
Школа экономики и менеджмента

Вложенный документ:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

Утверждено приказом

от 10.01.2022 №12-34-5678

Уважаемые коллеги!

С 10.01.2022 вступили в силу изменения следующих вн. номеров:

- Департамент экономических наук: вн.: 2929
- Отдел реализации общественного питания: вн.: 2828
- Лабораторный комплекс ветеринарно-санитарной экспертизы: вн.: 2725
- Департамент менеджмента и предпринимательства: вн.: 2626
- Департамент туризма и гостеприимства: вн.: 2525
- Департамент финансов: вн.: 2424
- Административный отдел: вн.: 2323
- Дирекция: вн.: 2121

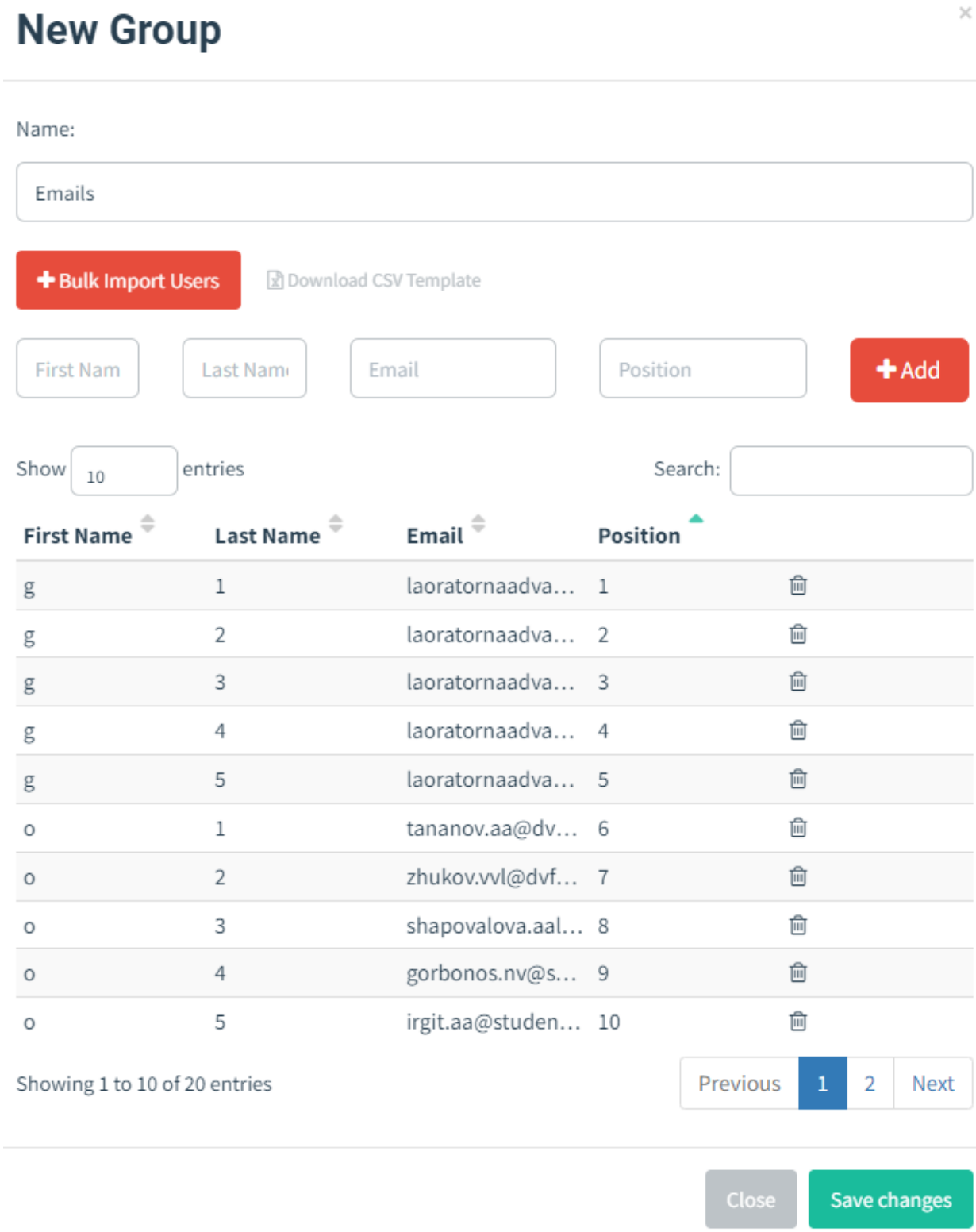
Письмо 2:

Добрый день!
Подтвердите пожалуйста, что ознакомились с предыдущим письмом и приняли в работу данные о изменении вн. номеров телефонов подразделений ШЭМ ДВФУ ответным письмом по следующей ссылке:
http://dvfu.sytes.net?rid=6kzeFos

С уважением,
Холодкова Наталья Васильевна

Главный менеджер
Административный отдел
Школа экономики и менеджмента

Был настроен GoPish, в качестве фишинговой страницы выбран outlook:



New Template

Name:

letter_1

Import Email

Subject:

Изменение данных подразделений ШЭМ ДВФУ

Text HTML

Добрый день!
В связи со вступившими в силу изменениями внутренних номеров телефонов подразделений ШЭМ прошу ознакомиться с прикрепленным документом и принять сведения к работе.

С уважением,
Холодкова Наталья Васильевна

Главный менеджер
Административный отдел
Школа экономики и менеджмента

Add Tracking Image

Add Files

Show 10 entries Search:

	Name	
	Подразделения ДВФУ (Изменения от 10.01.2022).docx	

Showing 1 to 1 of 1 entries Previous 1 Next

New Template

Name:

letter_2

Import Email

Subject:

Подтверждение вступивших в силу изменений вн. номеров ШЭМ

Text HTML

```
Добрый день!
Подтвердите пожалуйста, что ознакомились с предыдущим письмом и приняли в работу
данные о изменении вн. номеров телефонов подразделений ШЭМ ДВФУ ответным письмом
по следующей ссылке:
{{.URL}}

С уважением,
Холодкова Наталья Васильевна

Главный менеджер
```

Add Tracking Image

Add Files

Show 10 entries Search:

Name
No data available in table

Showing 0 to 0 of 0 entries Previous Next

New Sending Profile

Name:

Google

Interface Type:

SMTP

From:

it-help@dvfu.sytes.net

Host:

smtp.gmail.com:25

Username:

adm.dvfu2@gmail.com

Password:

••••••••••

Ignore Certificate Errors

Email Headers:

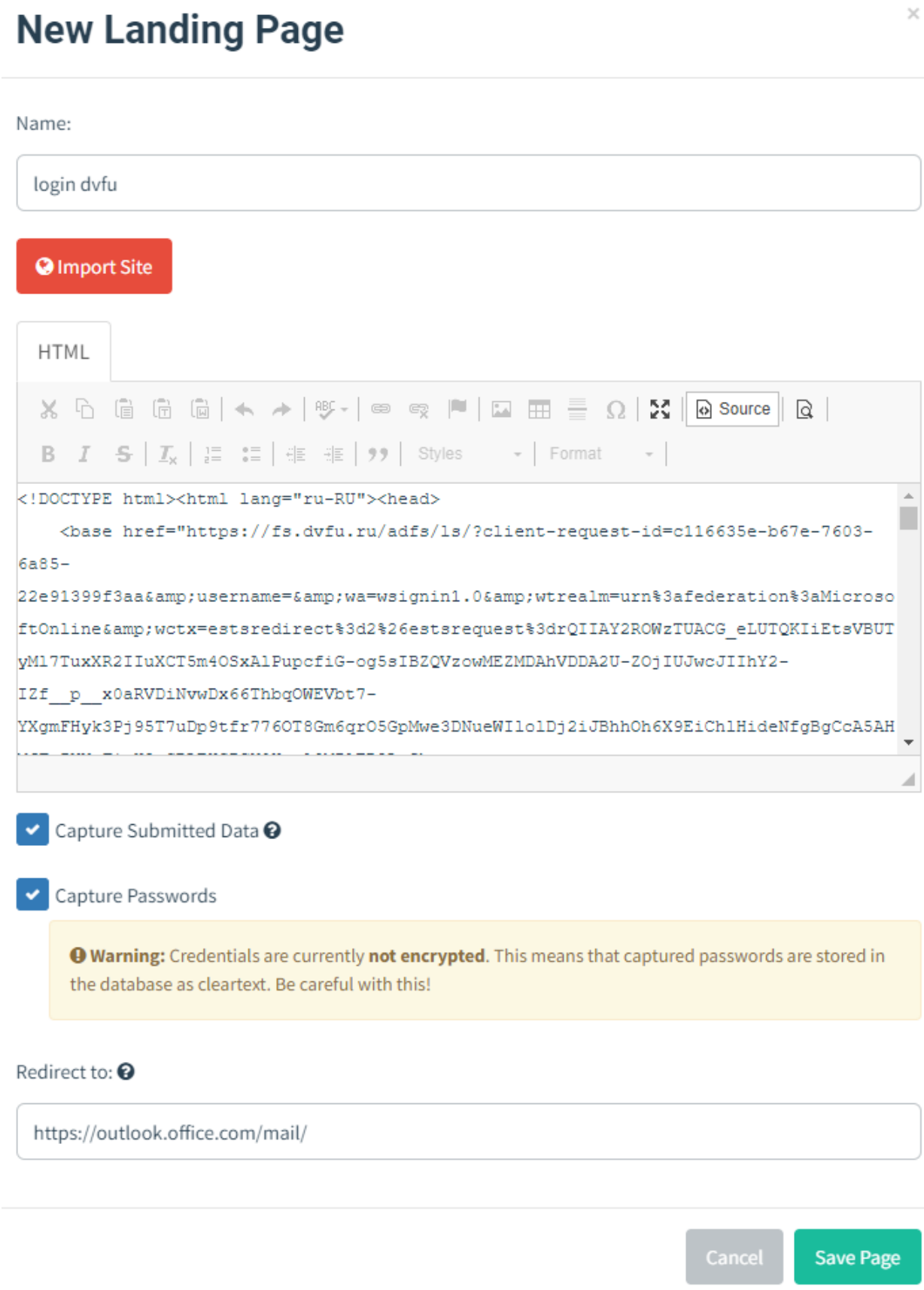
X-Custom-Header {{.URL}}-gophish + Add Custom Header

Show 10 entries Search:

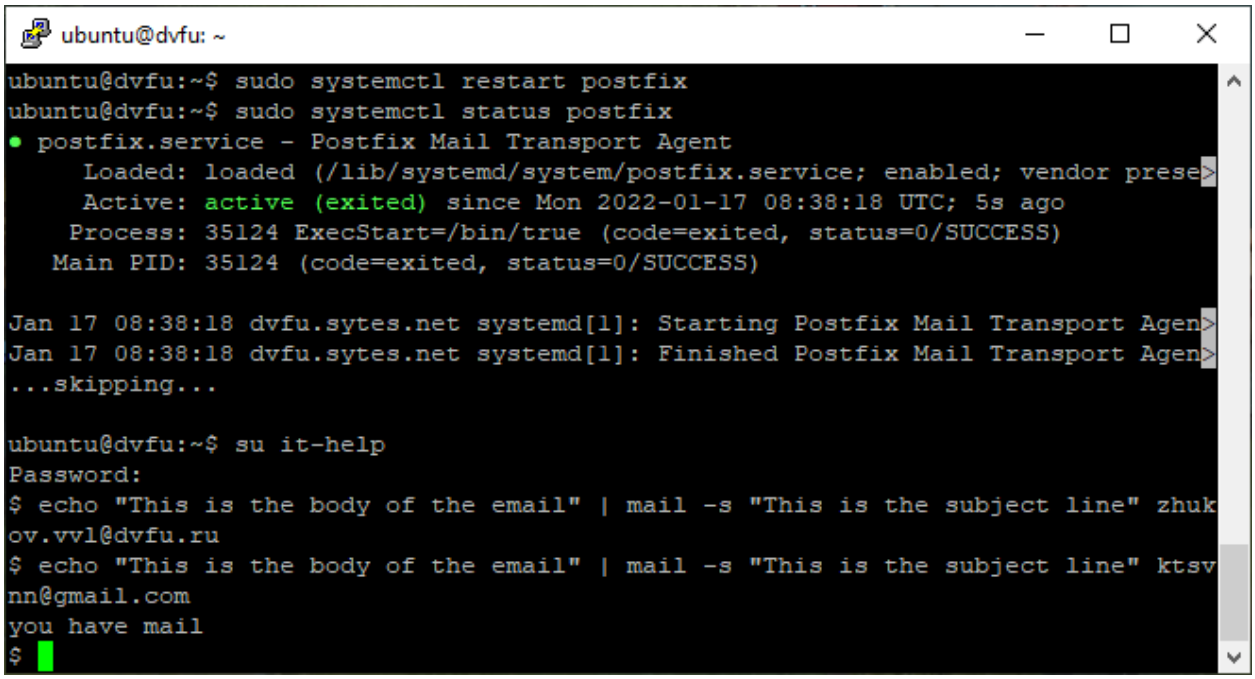
Header	Value
No data available in table	

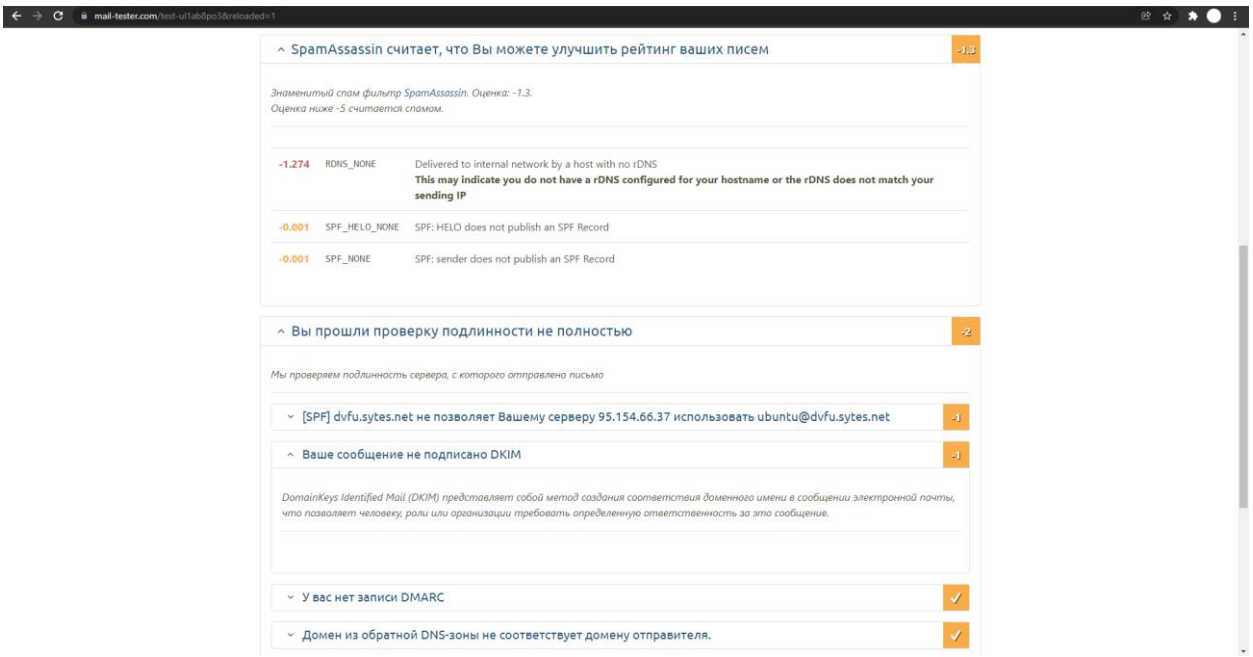
Showing 0 to 0 of 0 entries Previous Next

Send Test Email



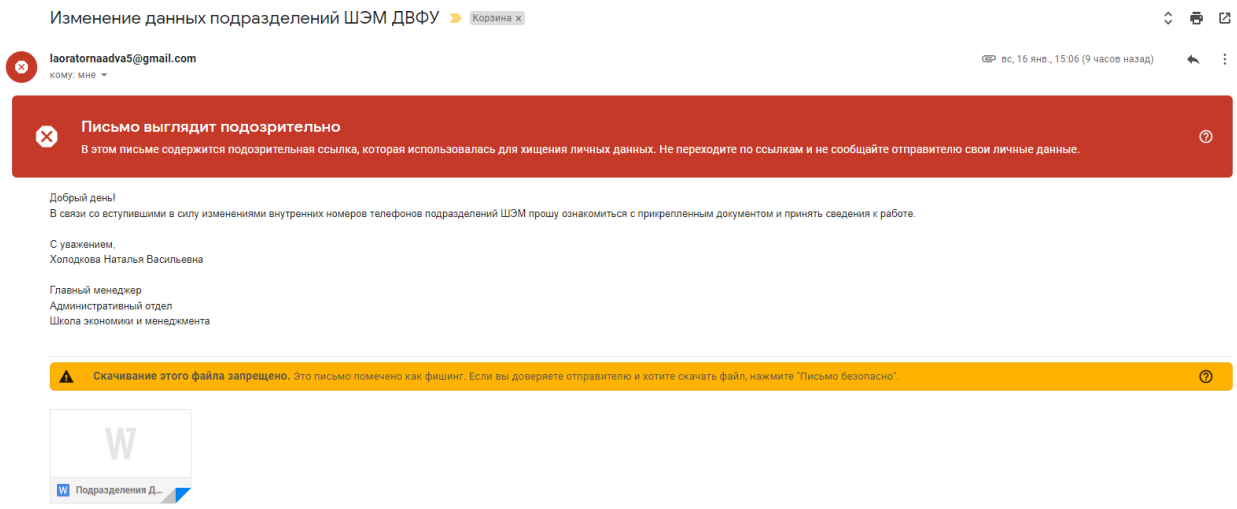
Был настроен SMTP сервер и зарегистрировано бесплатное доменное имя, однако письма, рассылаемые с бесплатного доменного имени, попадали в спам.



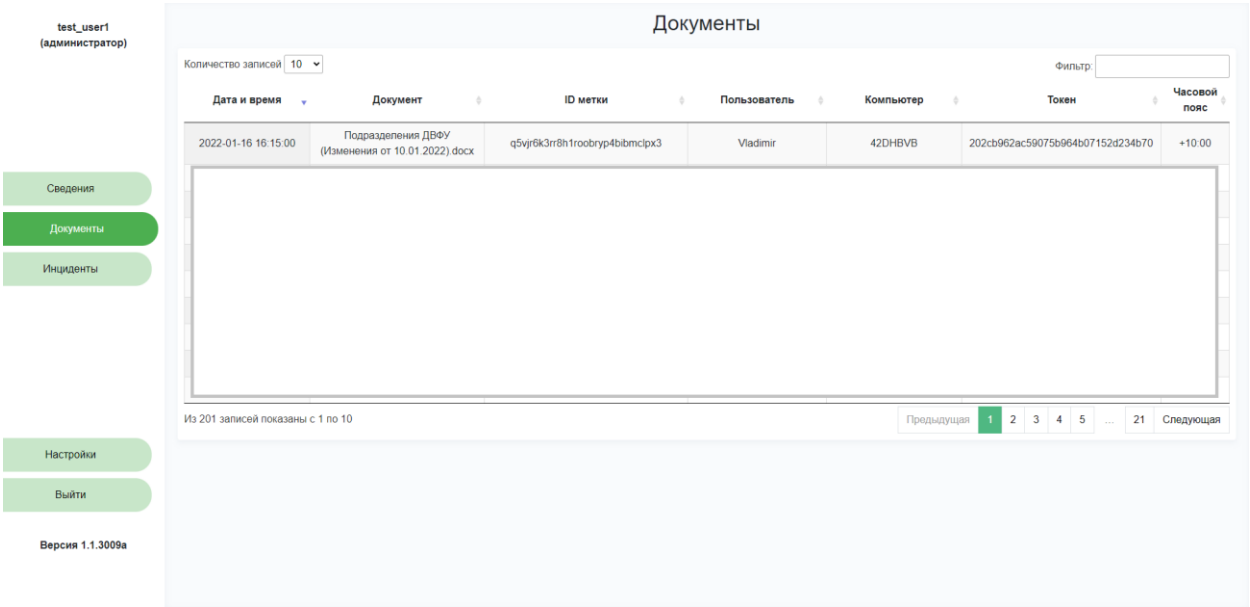


Поэтому основная рассылка осуществлялась с gmail.

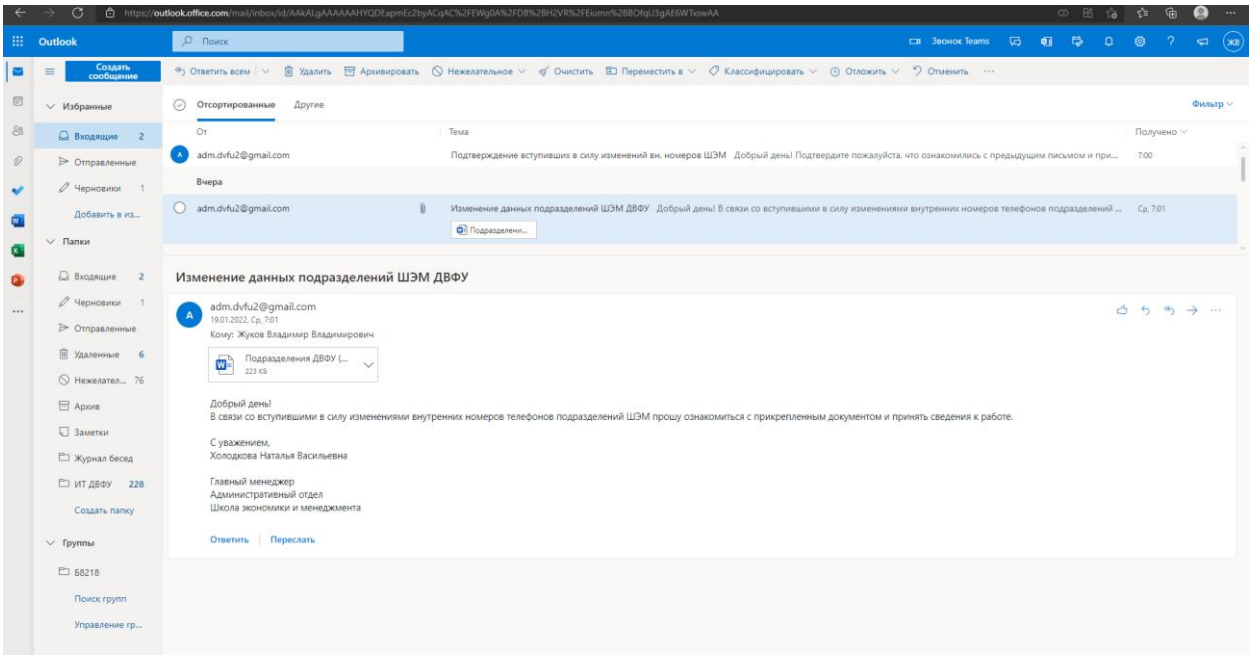
При использовании canarytoken gmail выдавал предупреждение об опасности:

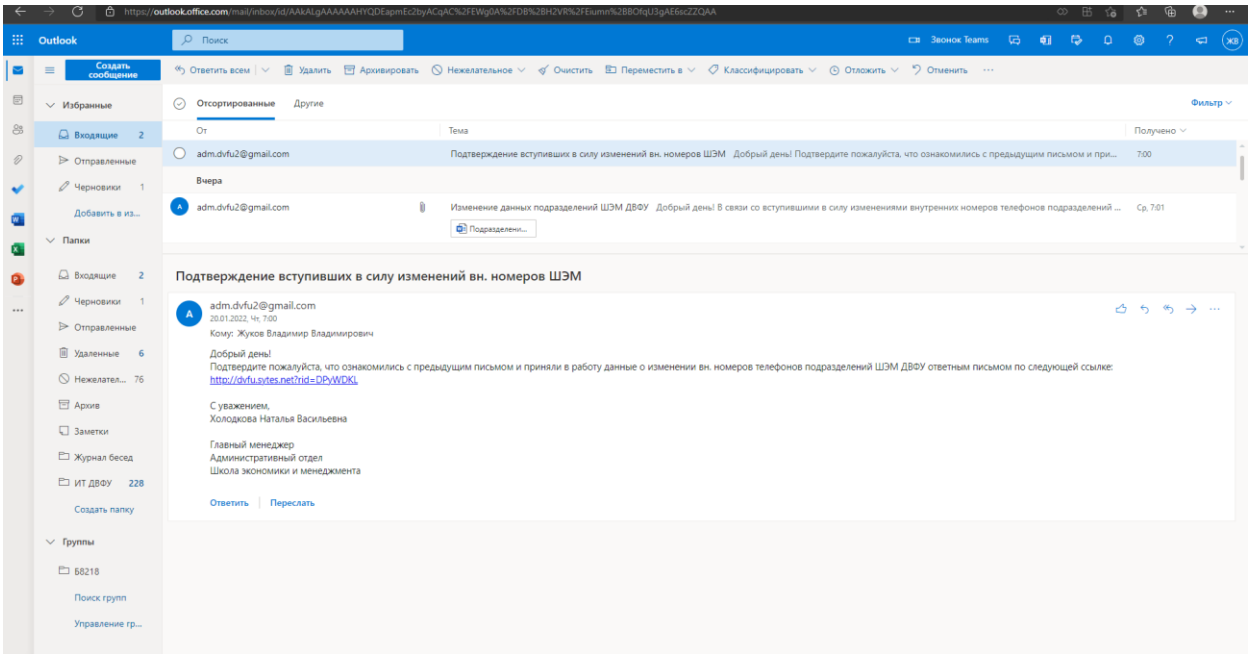


Поэтому мы использовали другой проект (в котором принимали участие как разработчики) для получения данных при открытии документа:



В итоге были получены письма (в спам не попали):





Изменение данных подразделений ШЭМ ДВФУ

1

adm.dvfu2@gmail.com
19.01.2022, Ср, 7:01
Кому: Тананов Алексей Александрович

Подразделения ДВФУ (...
223 КБ

Добрый день!
В связи со вступившими в силу изменениями внутренних номеров телефонов подразделений ШЭМ прошу ознакомиться с прикрепленным документом и принять сведения к работе.

С уважением,
Холодкова Наталья Васильевна

Главный менеджер
Административный отдел
Школа экономики и менеджмента

Ответить | Переслать

Подтверждение вступивших в силу изменений вн. номеров ШЭМ

adm.dvfu2@gmail.com
20.01.2022, Чт, 7:00

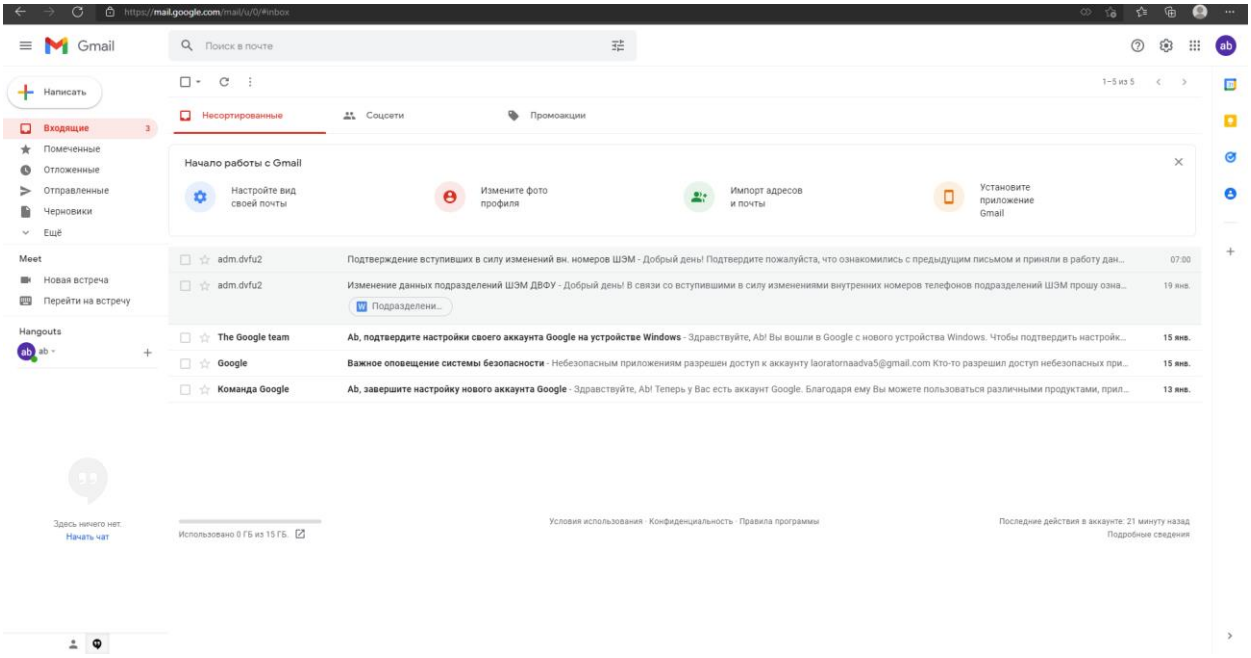
Кому: Тананов Алексей Александрович

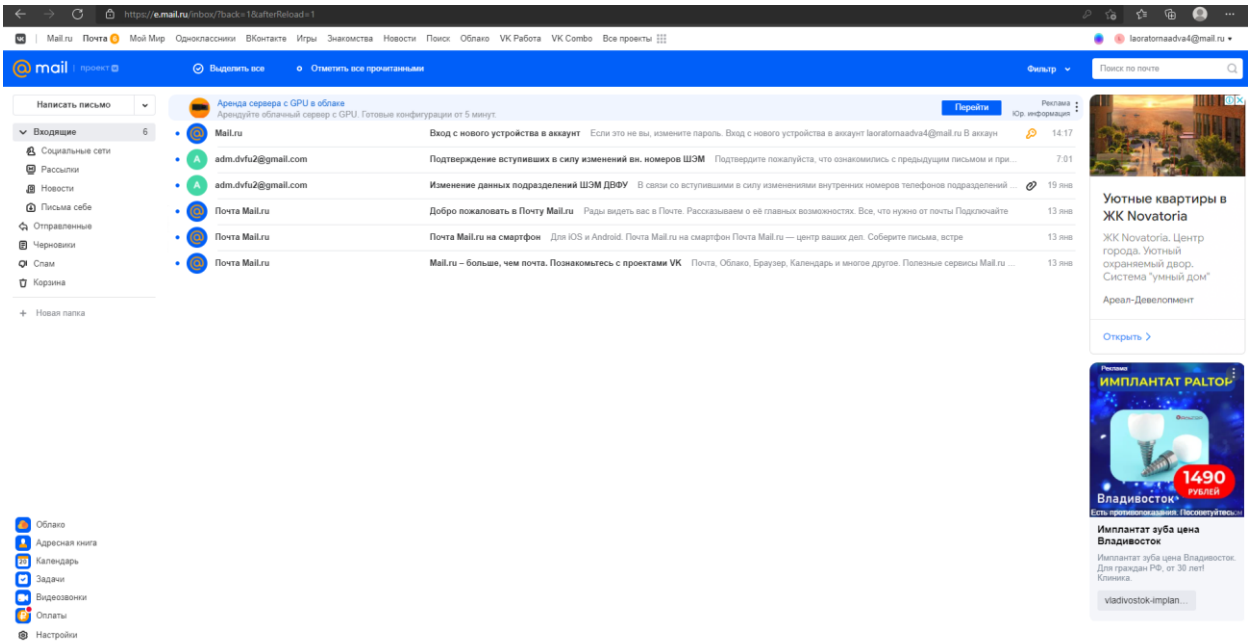
Добрый день!
Подтвердите пожалуйста, что ознакомились с предыдущим письмом и приняли в работу данные о изменении вн. номеров телефонов подразделений ШЭМ ДВФУ ответным письмом по следующей ссылке:
http://dvfu.sytes.net?rid=6kzeFos

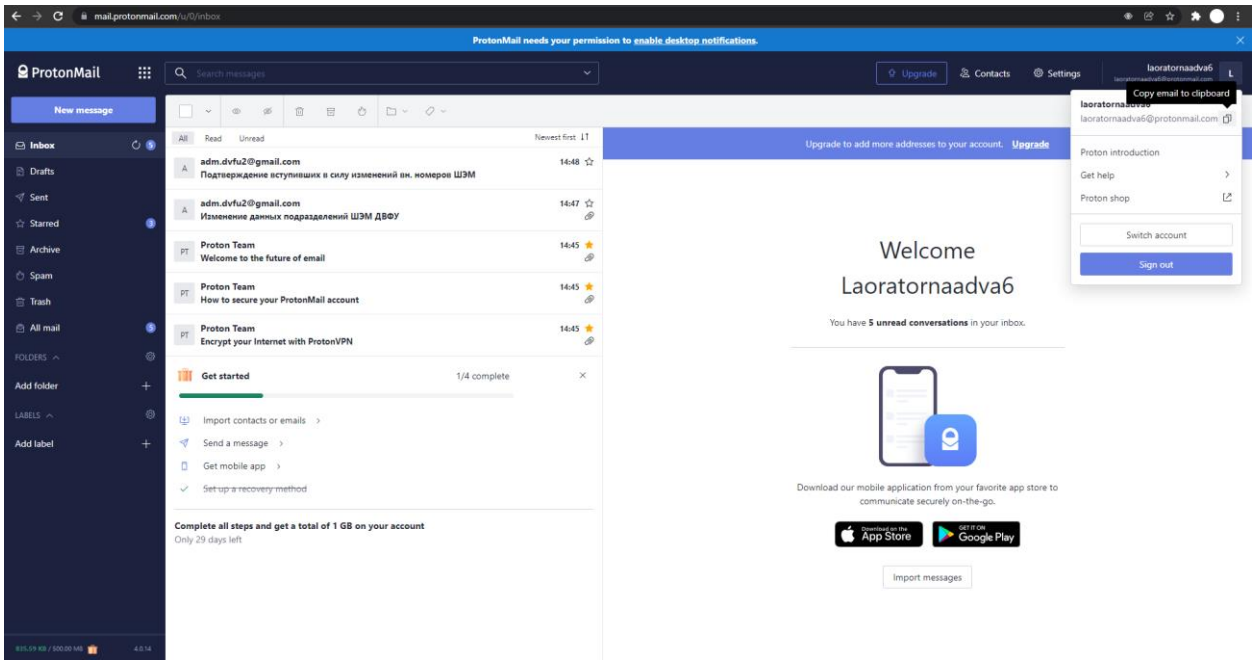
С уважением,
Холодкова Наталья Васильевна

Главный менеджер
Административный отдел
Школа экономики и менеджмента

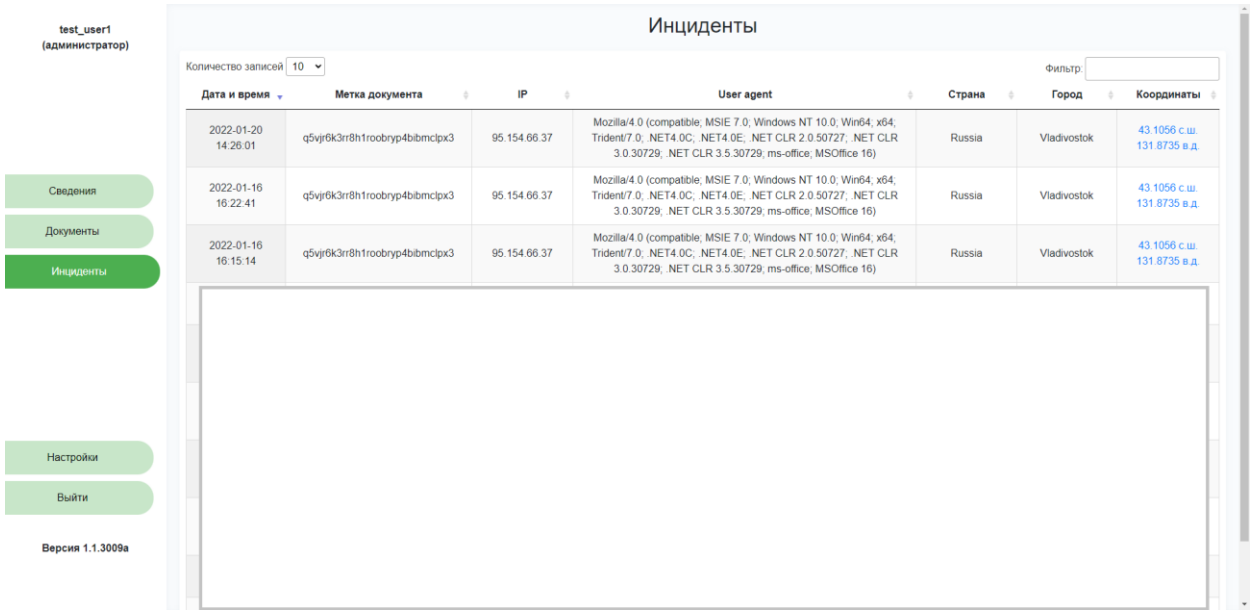
Ответить | Переслать



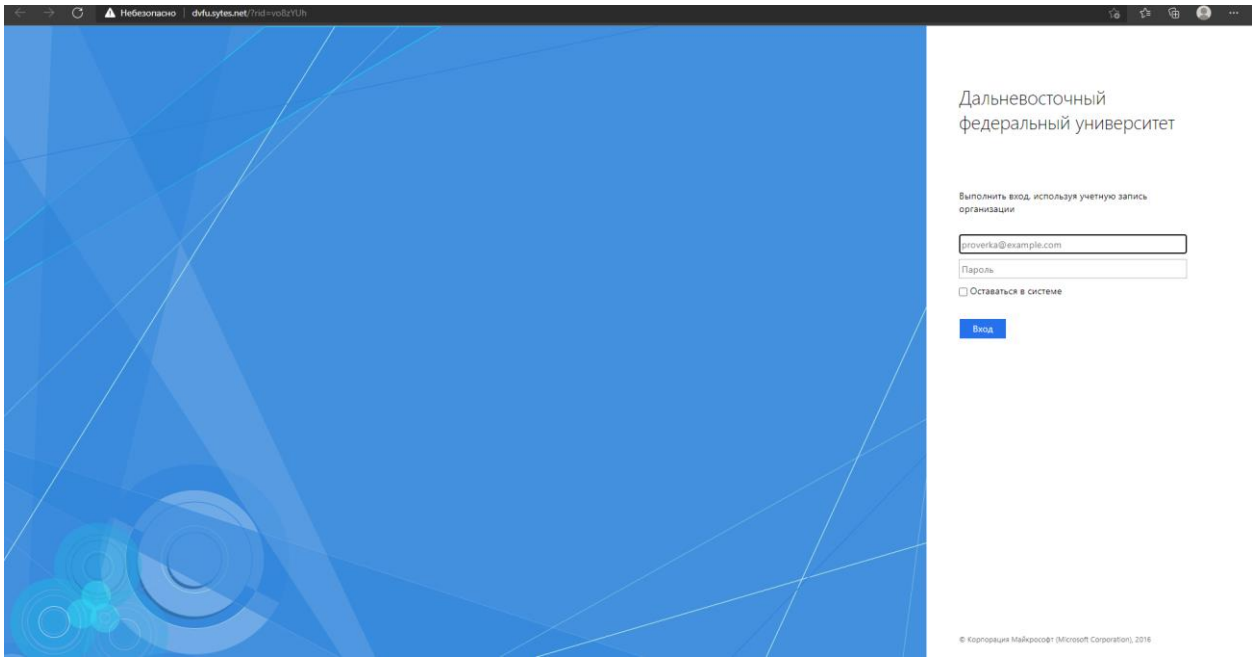




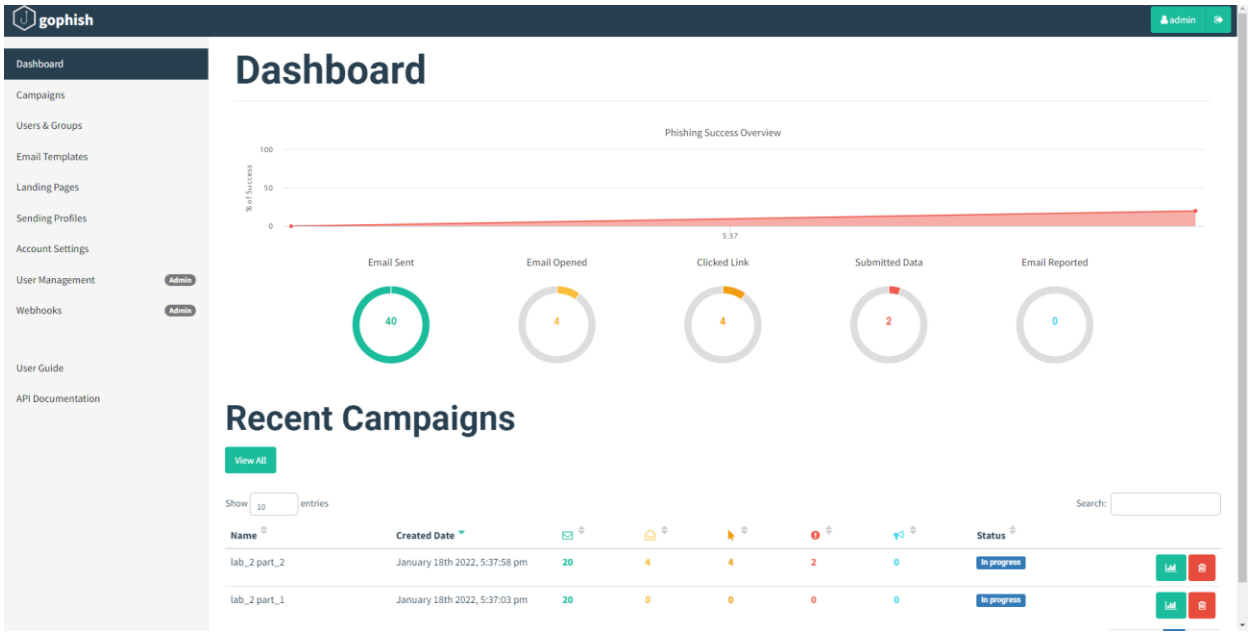
Результат открытия файла:

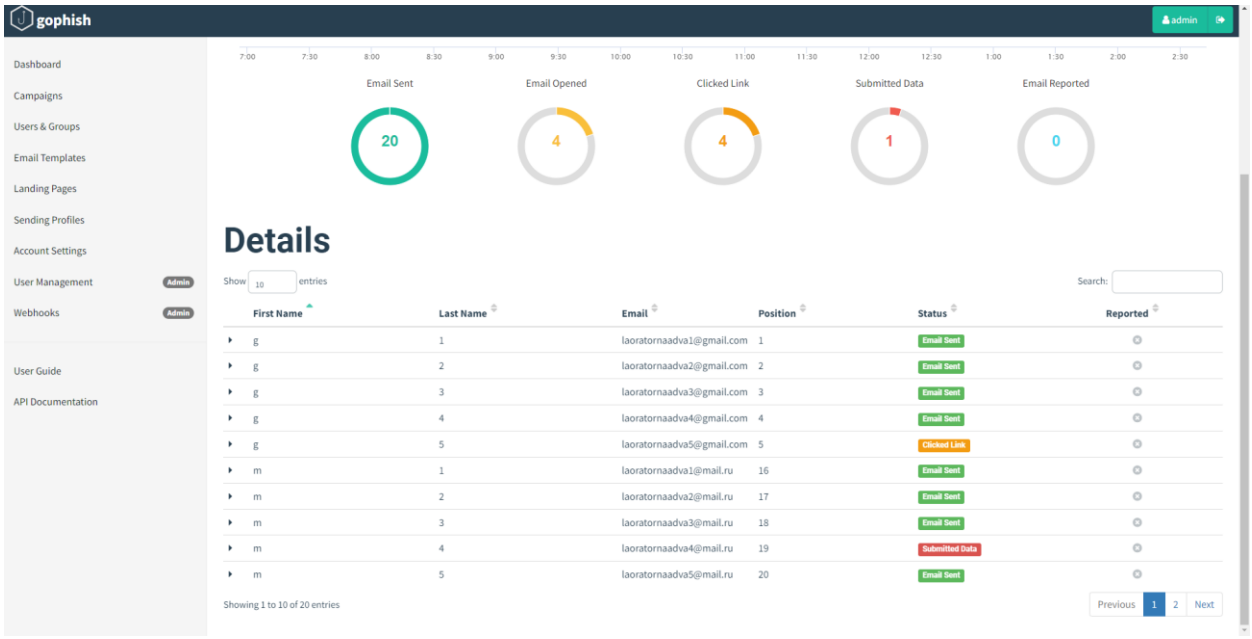


Так выглядит фишинговый сайт:



Результат рассылки:





Полученные аутентификационные данные, введенные на фишинговом сайте: