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

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Департамент информационной безопасности

Гусев Михаил Дмитриевич
Кудрявцева Юлия Андреевна
Увакин Данил Павлович

М9120-09.04.02ИБКФС

Отчет к лабораторной работе № 2
Проведение фишинговой атаки

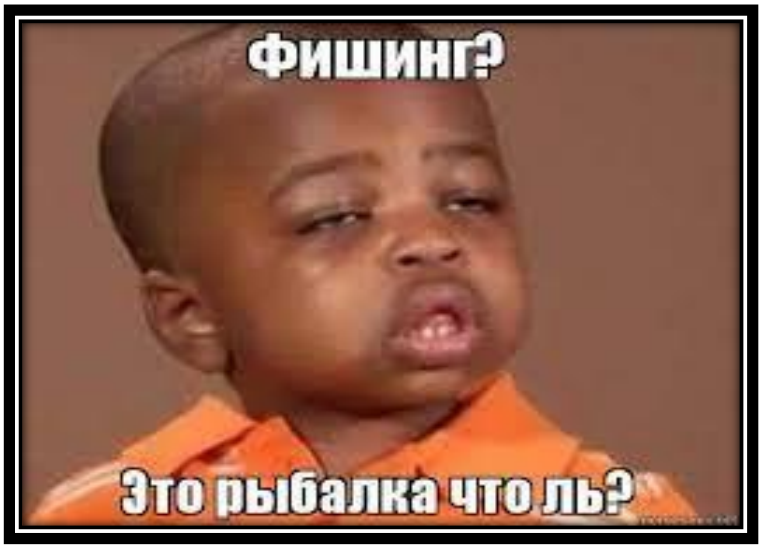
по дисциплине: «Аудит безопасности информационных систем»

г. Владивосток

2022

Задание:

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

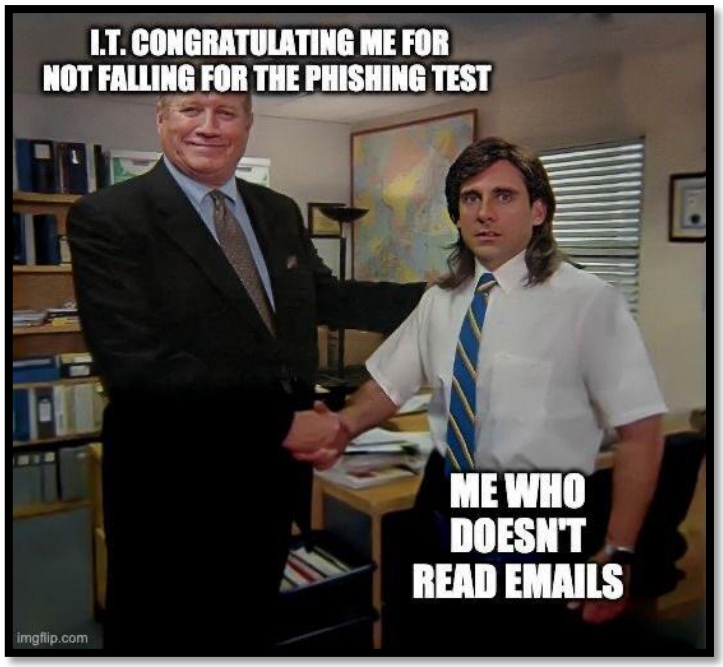
Для каждой из почт, описанных в начале, необходимо создать как минимум 5 аккаунтов, кроме почты ДВФУ. Данные почты, на которые проводятся атака, являются общими для всей группы. Почты ДВФУ, на которые проводятся атаки, должны быть личными почтами группы, также в количестве 5 штук.

Почты ДВФУ для получения фишинговых ссылок могут быть разными для каждой из выполняющих задание групп, почты предоставляют одногруппники. В отчете должны быть скрины полученных писем и куда они попали (спам или нет), предоставлять пару логин:пароль запрещено для почт ДВФУ, по этому заранее договоритесь с одногруппниками, на почты которых будут приходить фишинговые письма, чтобы они предоставили вам все скрины после получения письма. Для почт gmail.com, mail.ru protonmail.com создать общий пул почт с кредами login:pass.

Лабораторная работа выполняется с использованием фреймворка GoPhish (https://getgophish.com/,https://github.com/gophish/gophish)

Для проведения фишинговой компании необходимо настроить SMTP сервер и поднять фейковую фишинговую страницу ресурса (на выбор из пункта 2 критерий). Фейковая страница создается через GoPhish (необходимо доменное имя).

После перехода на фишинговый сайт, пользователь должен увидеть форму авторизации, после этого должны быть введены данные в поле логина ФИО, в поле пароля текущая дата и время в формате ГГГГ.ММ.ДД.ЧАС.МИН.



Для создания фишинговой компании в GoPhish необходимо зарегистрировать бесплатное доменное имя. Для лабораторной можно приобрести собственное доменное имя, если не хотите использовать бесплатное. Для писем, содержащих файл необходимо настроить сервер, который будет принимать информацию, полученную от открытого документа. Отключать антивирус при открытии файла нельзя.

Требование к отчету по лабораторной работе:

В отчете должны быть отражены скрины с описанием создания и проведения фишинговой компании, создания SMTP сервера и результаты открытия писем, файлов и переходов на фишинговые ресурсы, с указанием того, попало ли письмо в папку спам и информацией о введенных кредах. Отчет должен быть в формате pdf или md.

Введение

Почты:

aristocrat1998@gmail.com: pwd
luckyaki1998@gmail.com: pwd
gusev.miha2011@gmail.com: pwd
sukasobaka77@gmail.com: pwd
uliakudriavtceva@gmail.com: pwd
tihonova.ts.dvfu@gmail.com : pwd

uvakin.dp@mail.ru : pwd
ifqtjndxp@mail.ru: pwd
kudriavtcevayuliya98@mail.ru: pwd
gusev-miha2011@mail.ru : pwd
tfhbdfddf@mail.ru: pwd

yan.ju.li@protonmail.com: pwd
arkadiinemoy@protonmail.com: pwd
kudjuli@protonmail.com: pwd
zotovnyasha@protonmail.com: pwd
uliakudriavtceva@protonmail.com: pwd

gusev.md@students.dvfu.ru : pwd
uvakin.dp@students.dvfu.ru : pwd
kudryavtceva.ya@students.dvfu.ru : pwd
savelev.dv@students.dvfu.ru : pwd
penkin.ss@students.dvfu.ru : pwd

Тематика писем:

1 шаблон писем

Письмо содержит информацию

об изменении внутренних номеров

подразделений.

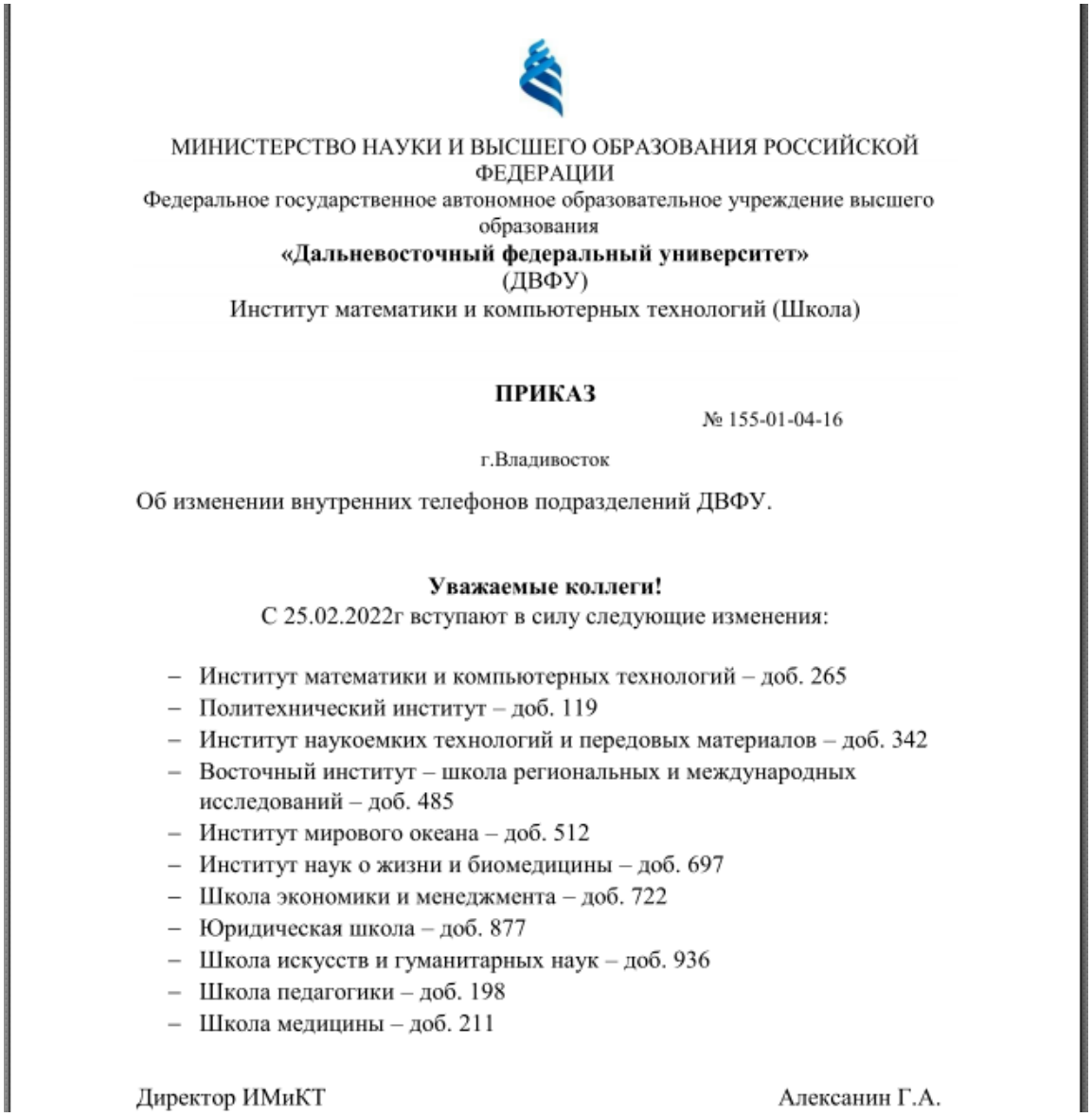
Письма отправлены от имени главного

специалиста:

Тихонова Татьяна Сергеевна

E-mail: tikhonova.ts.dvfu@outlook.com

SMTP сервер Outlook



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)
Институт математики и компьютерных технологий (Школа)

ПРИКАЗ

№ 155-01-04-16

г.Владивосток

Об изменении внутренних телефонов подразделений ДВФУ.

Уважаемые коллеги!
С 25.02.2022г вступают в силу следующие изменения:

- Институт математики и компьютерных технологий – доб. 265
- Политехнический институт – доб. 119
- Институт наукоемких технологий и передовых материалов – доб. 342
- Восточный институт – школа региональных и международных исследований – доб. 485
- Институт мирового океана – доб. 512
- Институт наук о жизни и биомедицины – доб. 697
- Школа экономики и менеджмента – доб. 722
- Юридическая школа – доб. 877
- Школа искусств и гуманитарных наук – доб. 936
- Школа педагогики – доб. 198
- Школа медицины – доб. 211

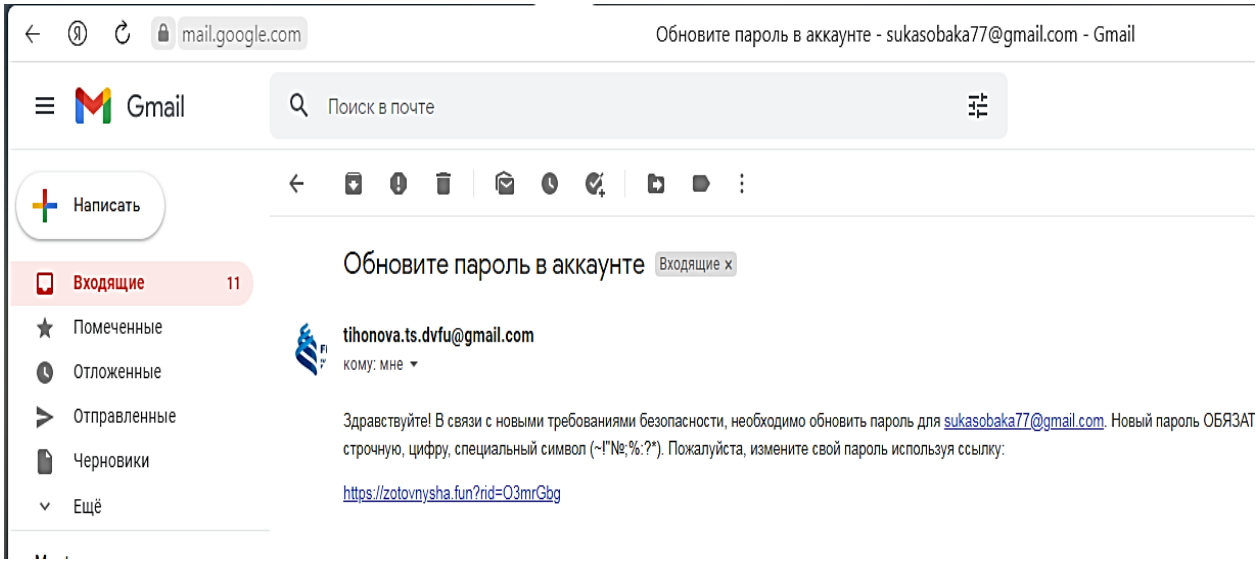
Директор ИМиКТ Алексанин Г.А.

2 шаблон писем

Требуется замена пароля для указанной почты

«Здравствуйте**!** В связи с новыми требованиями безопасности**,** необходимо обновить пароль для **{{.email}}** Новый пароль ОБЯЗАТЕЛЬНО должен содержать от **10** символов**,** включая минимум одну заглавную букву**,** строчную**,** цифру**,** специальный символ **(~!"№;%:?*).** Пожалуйста**,** измените свой пароль используя ссылку**:**

https://zotovnysha.fun?rid=O3mrGbg»



Письма также отправлены от имени главного специалиста:

Тихонова Татьяна Сергеевна

E-mail: tihonova.ts.dvfu@gmail.com

Здесь нами был использован SMTP сервер Гугл, а не Outlook,

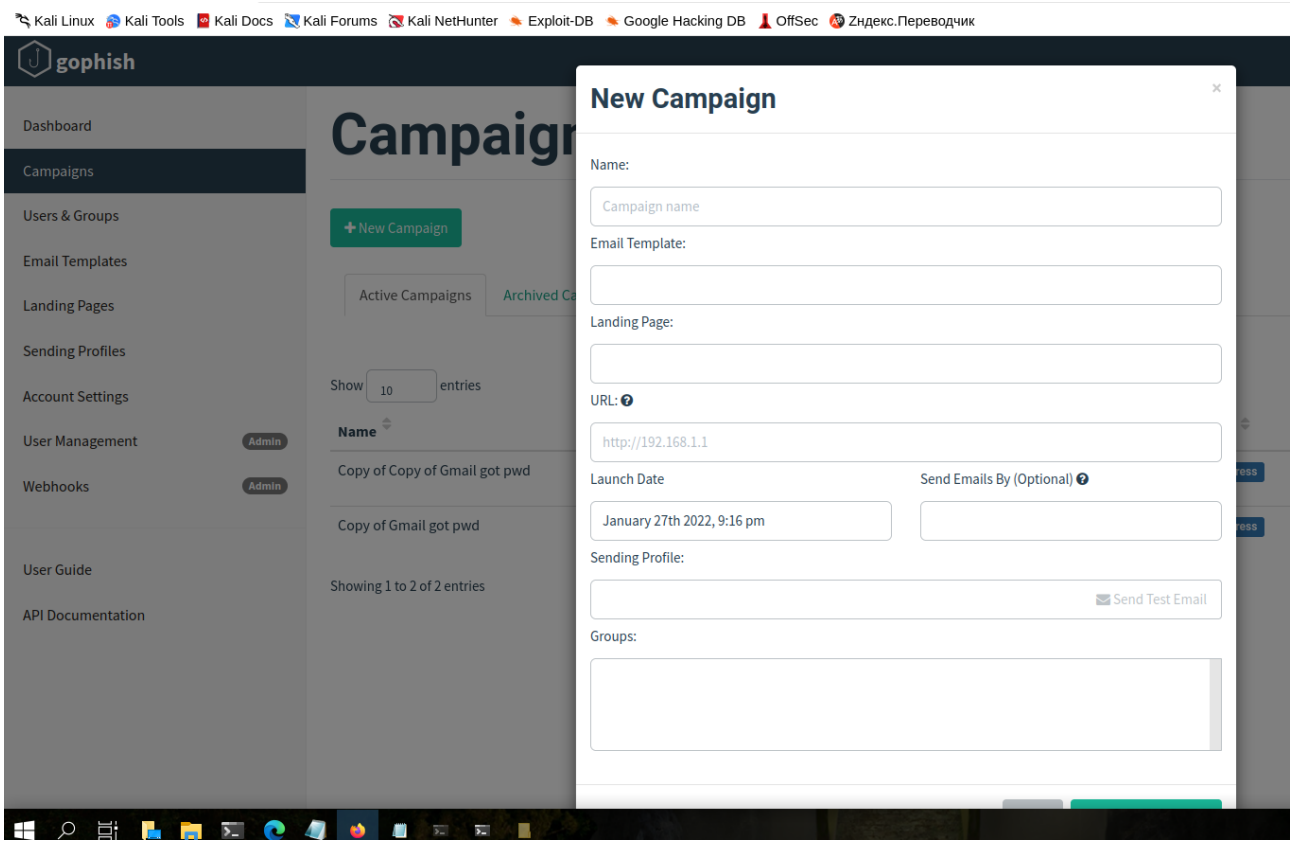
во имя и славу Разнообразия

Глава 1. Часть 1. Использование фреймворка GoPhish

И молвила глобальная сеть:

...Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing. This is an important tool for penetration testers and ethical hackers...

Первым делом, потренируемся с ~~удочкой~~ фреймворком локально, запустим на машине кали:



Видим, что нам нужно: шаблон письма, страница для ~~кражи~~ заимствования логинов и паролей, домен для размещения этой самой страницы, и тот, кто будет отправлять письма ~~(рыбак?).~~

Переходим к домену, но вовремя вспоминаем, что перед нами ещё стоит задача получить от писем информацию о системе, перешел ли пользователь по ссылке и введенной информации. Нужен сервер.

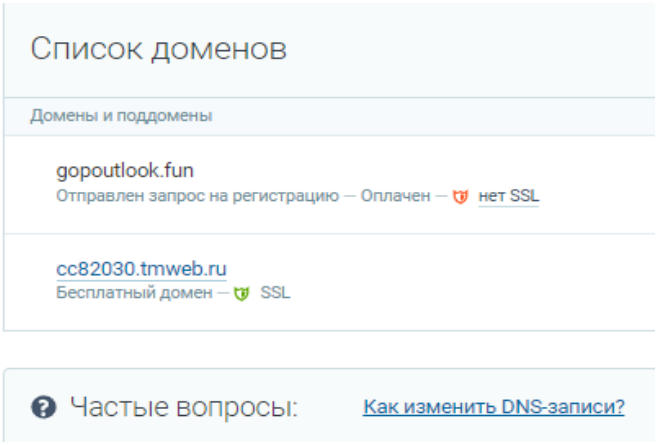
Часть 2 Первый опыт с поднятием сервера и домена

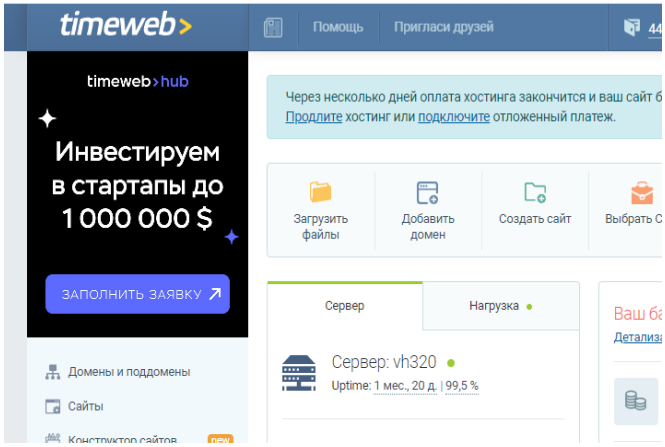
Первый блин комом © …народная мудрость

Настраиваем домен, сертификаты безопасности, хостинг.

И, естественно, сначала идем искать бесплатный домен и сервер.

Студенты мы или кто?





Спойлер: ограничения бесплатного сервера помешают нам сделать наше серое дело.

По прошествии 3 дней битв, истерик и поиска проблемы,

плюем на сыр в мышеловке,

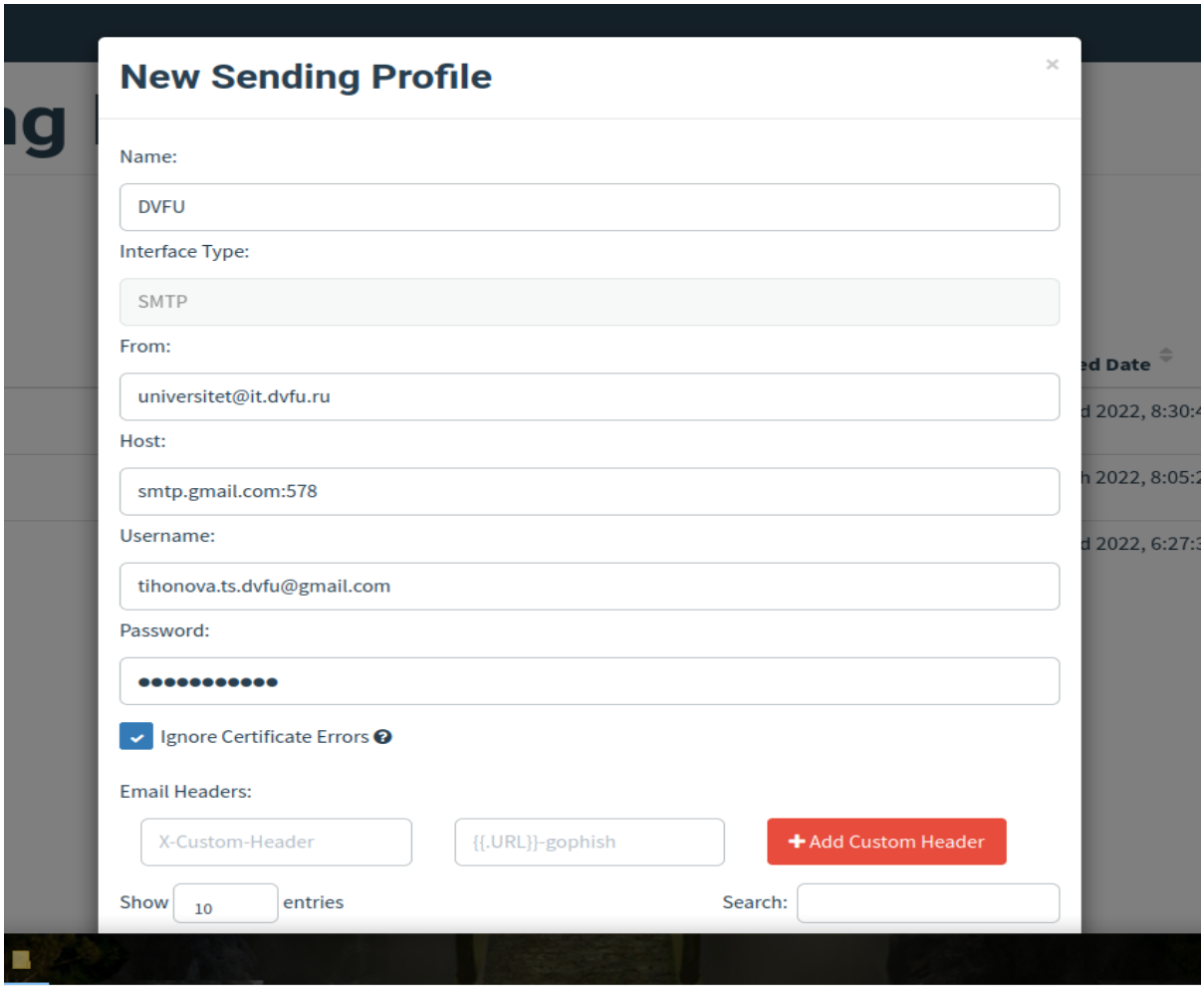
роняем слезу за потраченную сотку на прикольный домен и покупаем VPS у конкурентов.

Подключаем по ssh сервер, настраиваем сертификат SSL (благо бесплатно), переходим на https, ибо мы, как уважаемые люди, радеем за безопасность ^_^

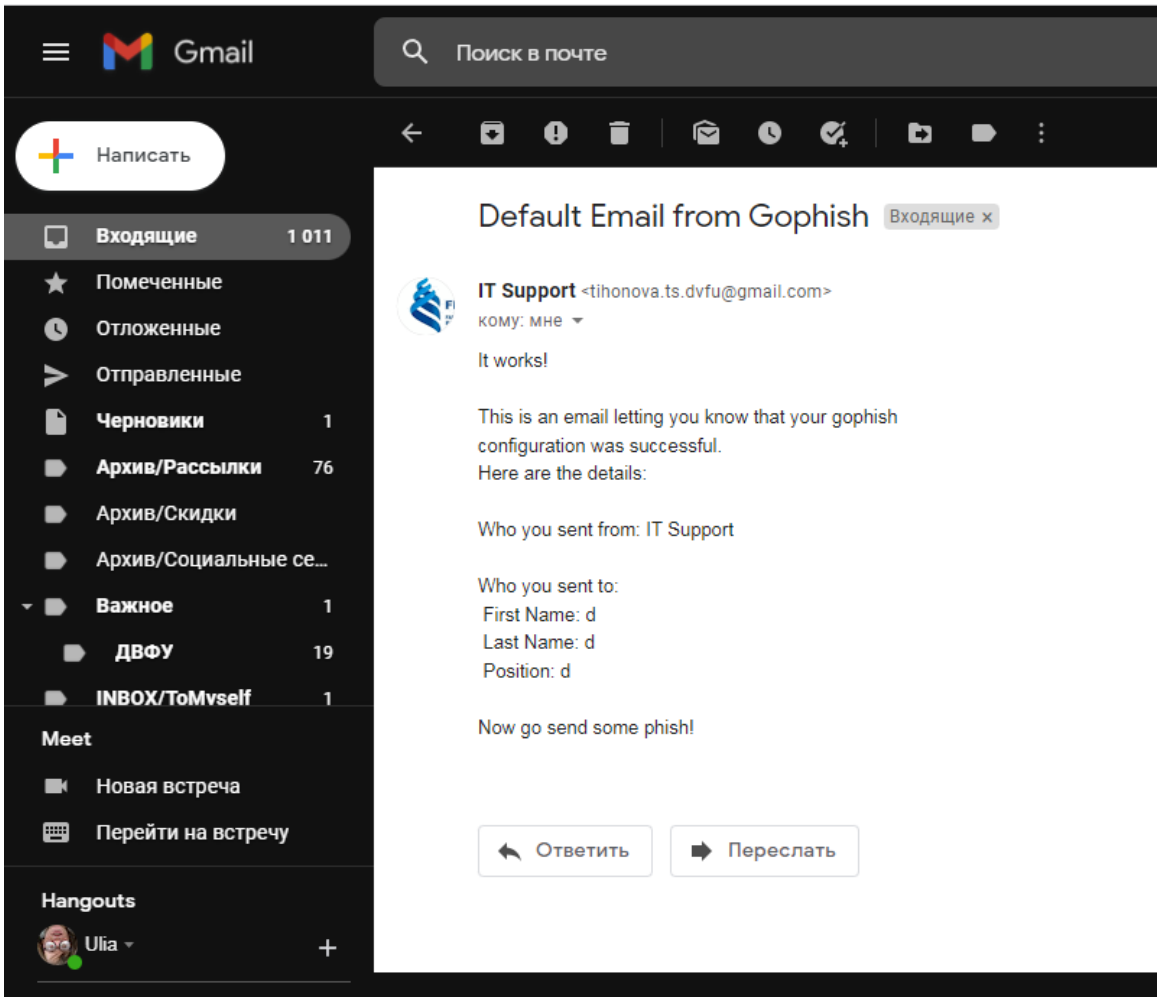
Делаем на него чудо-фреймворко-загружато и начинаем заполнение.

Глава 2 Часть 1 Особенности информационной рыбалки

Сначала готовим рыбака.

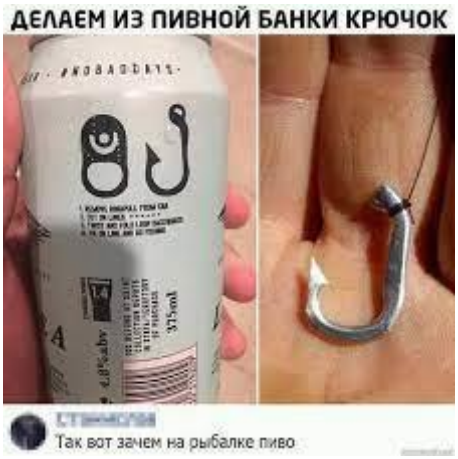


Настроили все, что от нас требовалось, проводим проверку аккаунта менеджера



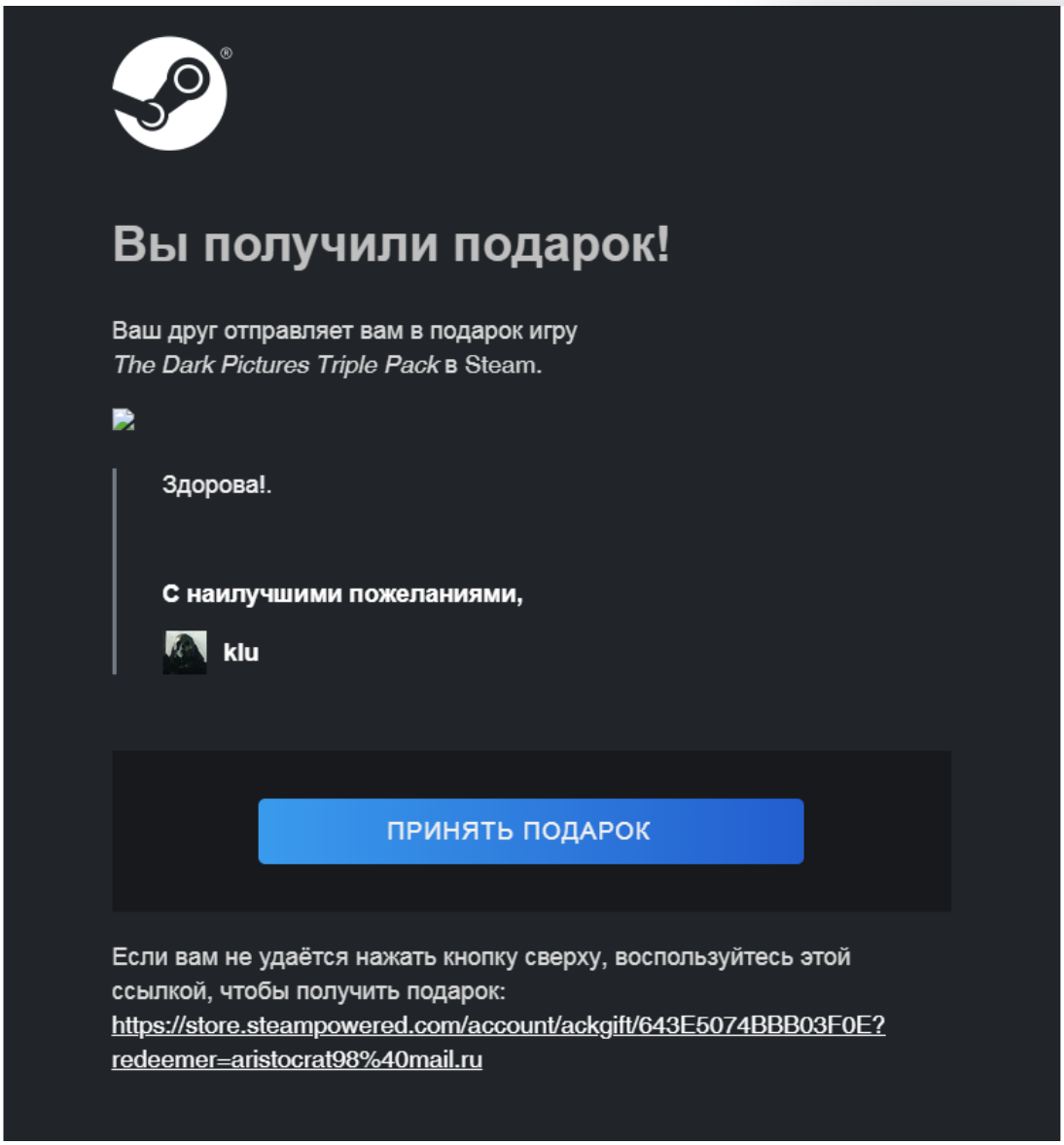
Далее ~~крючок с червячком~~ письма.

Письмо с документом встраиваем канарейку, сообщающую нам информацию о системе. Также, не забываем добавить отслеживающую картинку.

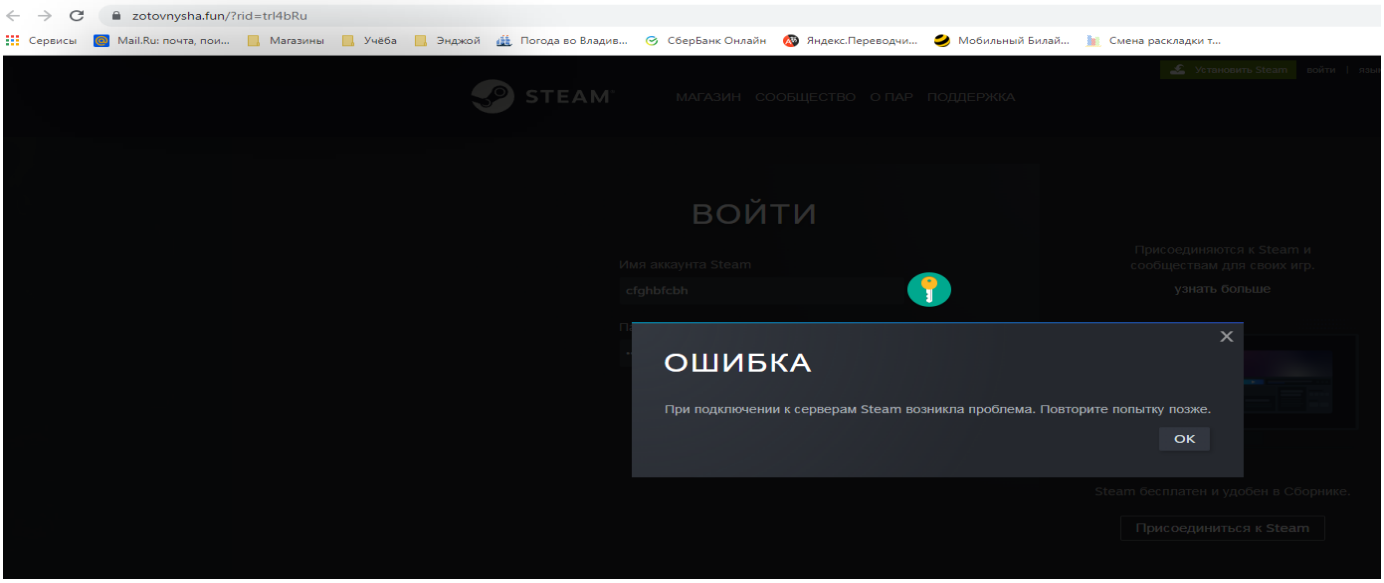


...И все могло бы пойти хорошо, но нет...

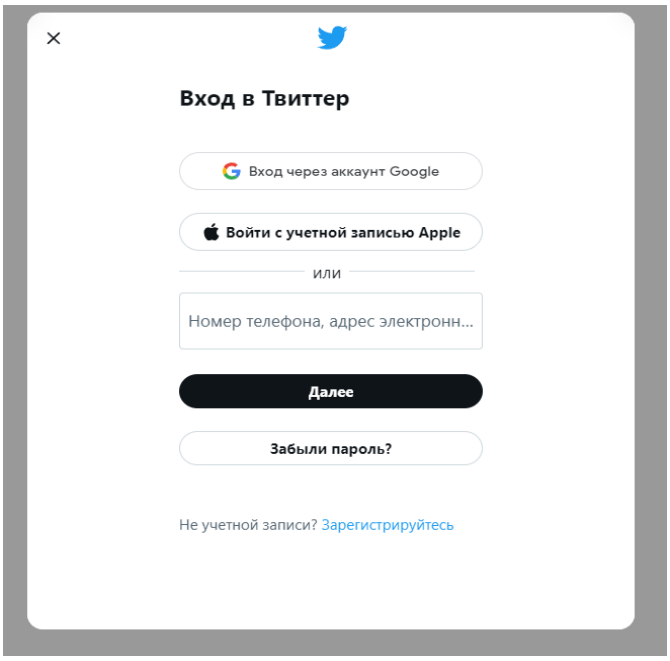
Здесь нас ждала засада. Не такая обидная как потеря сотки, но все же неприятная.
Мы подготовили письма-приманки для Steam, но попытки сделать его фишинговую страницу, а также нескольких других сервисов, провалились…



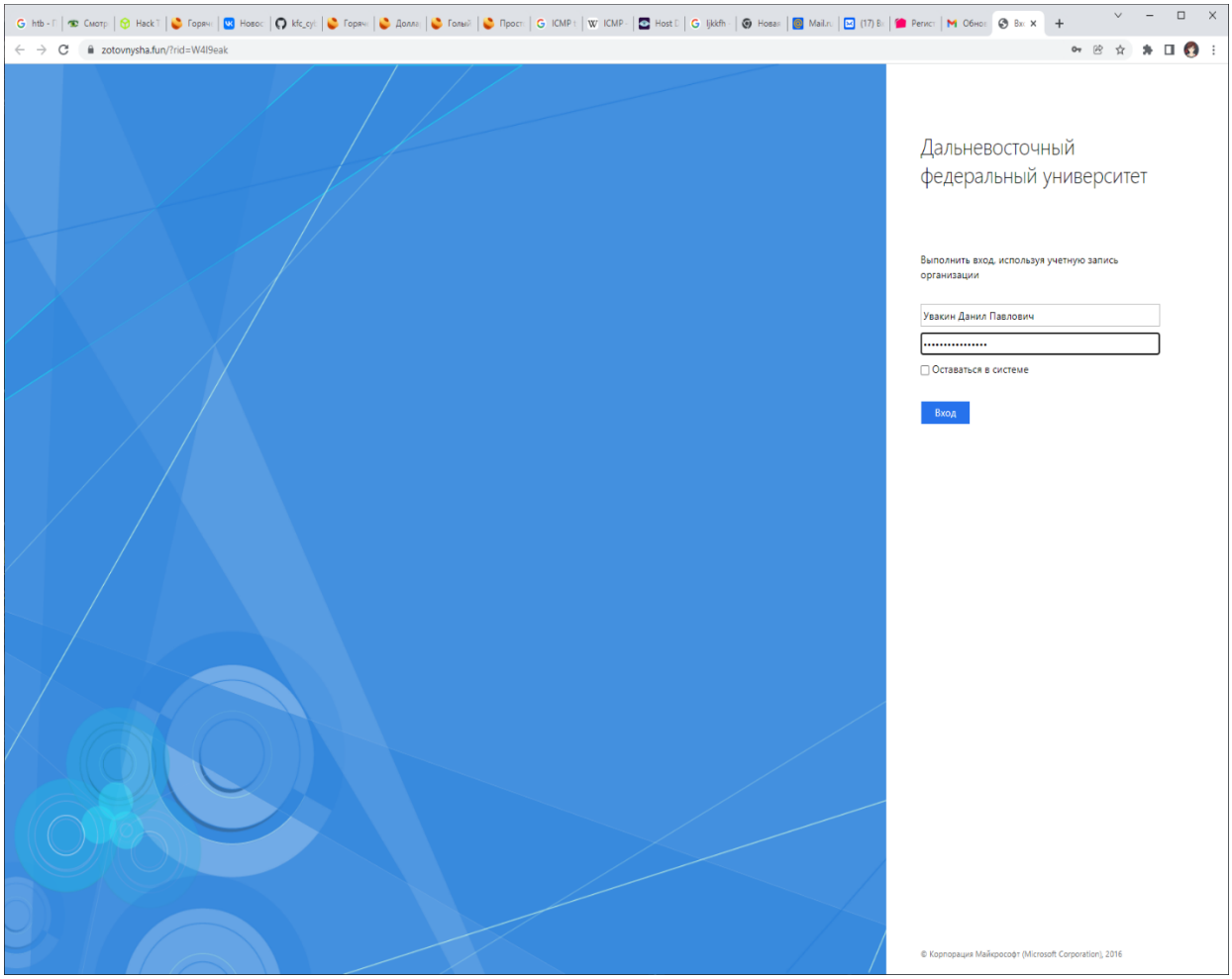
Поползновения сделать фишинговыми страницы Facebook и Google не дали желаемого результата. Сайты мешают Gophish получить введенную пользователем информацию.



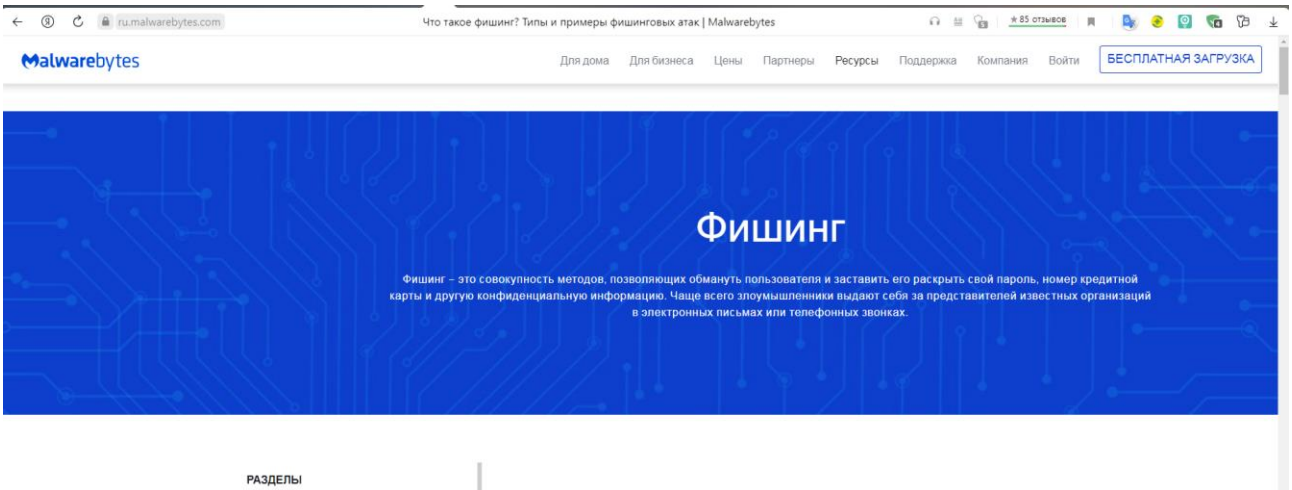
А Twitter и mail.ru построены так, чтобы разделить логин и пароль на разные страницы.



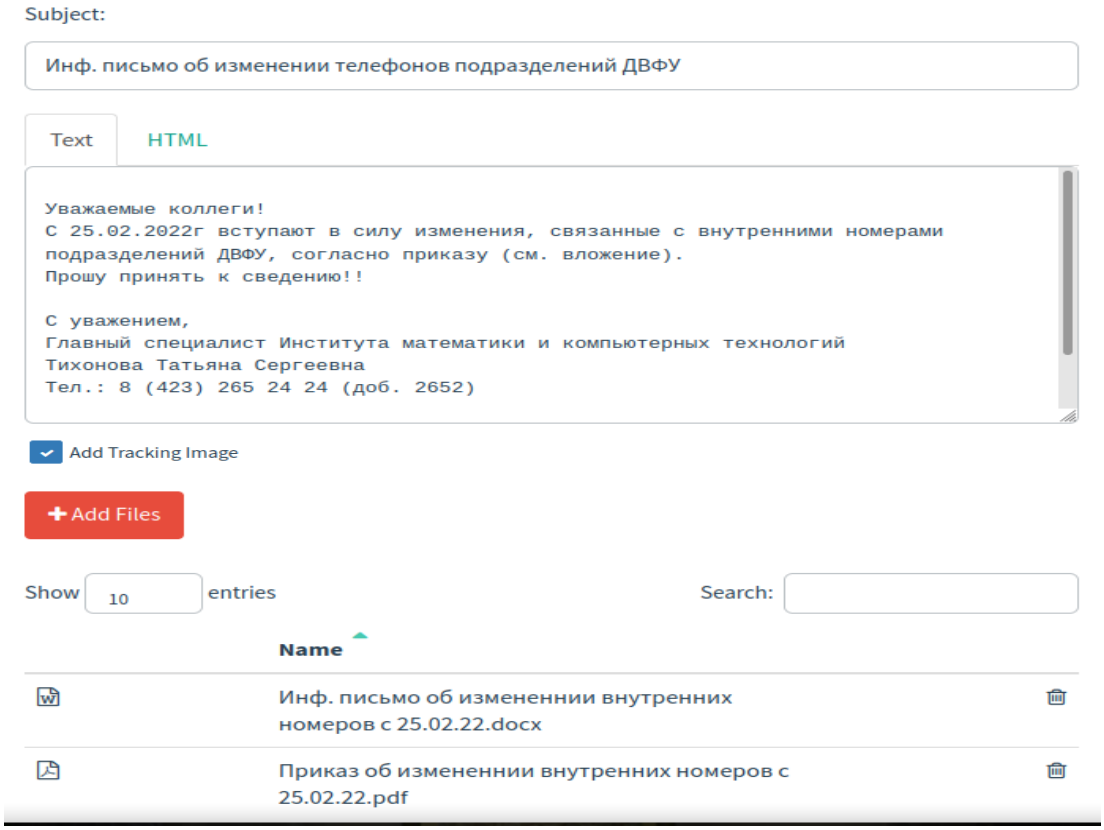
И здесь нас выручают ДВФУ и Outlook!



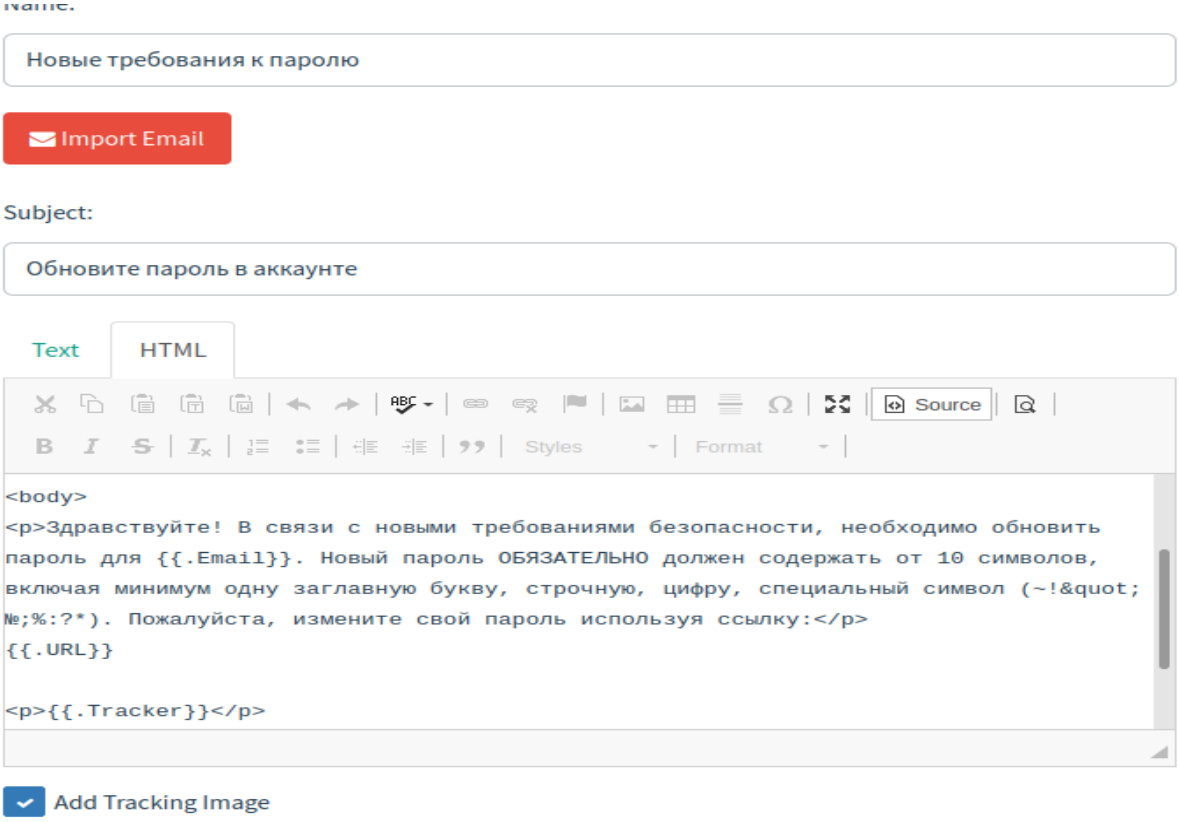
Даже работает перенаправление после введения данных. Красота



Поэтому делаем письма в тематике ДВФУ.



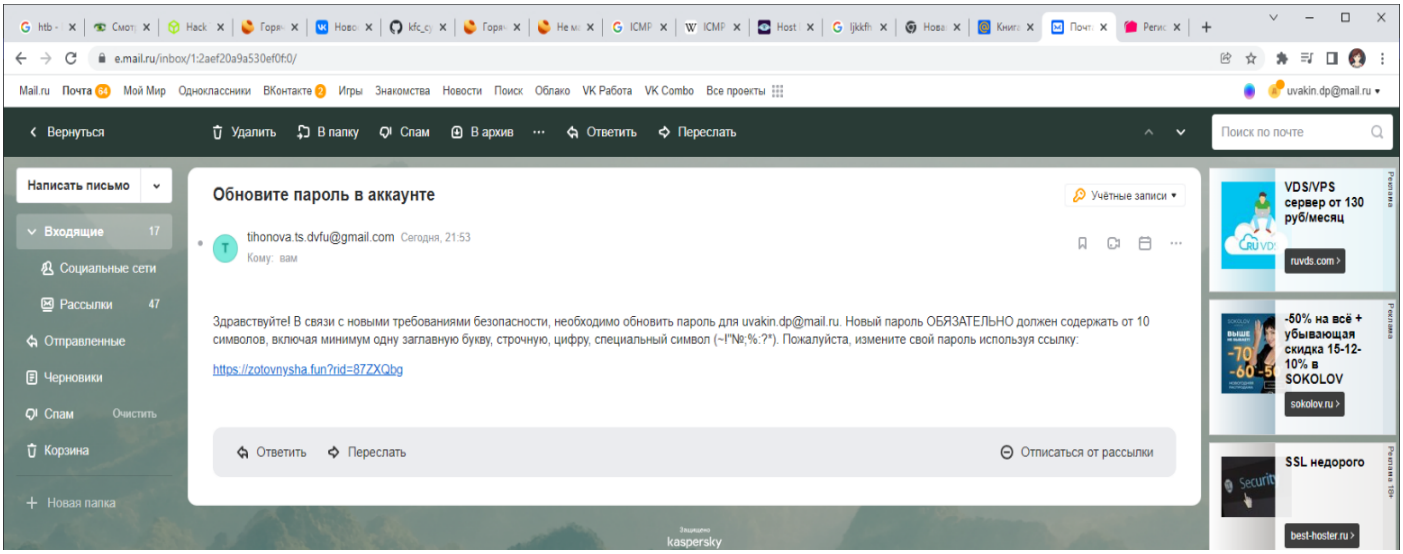
Письмо с ссылкой:

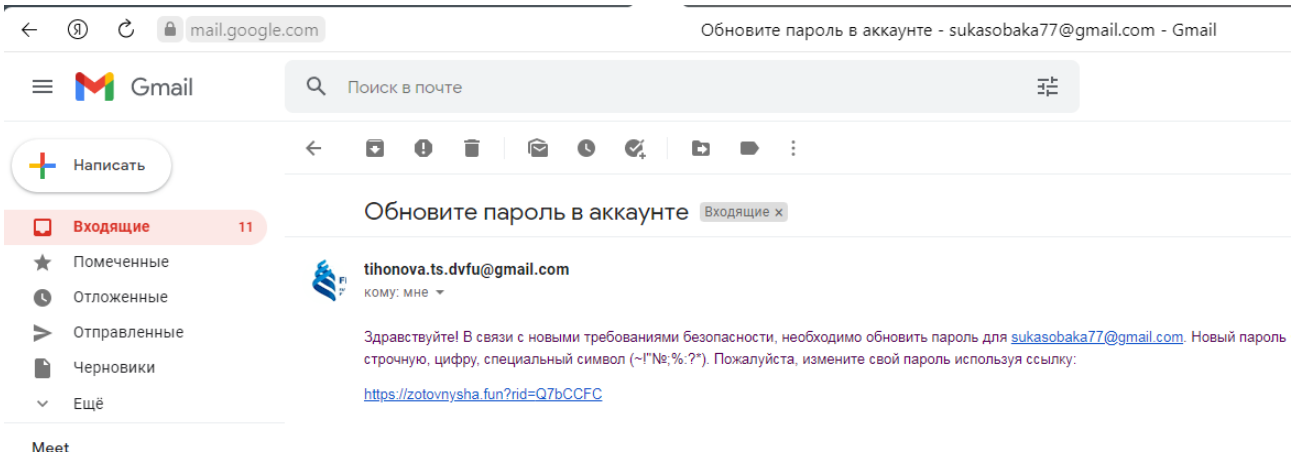


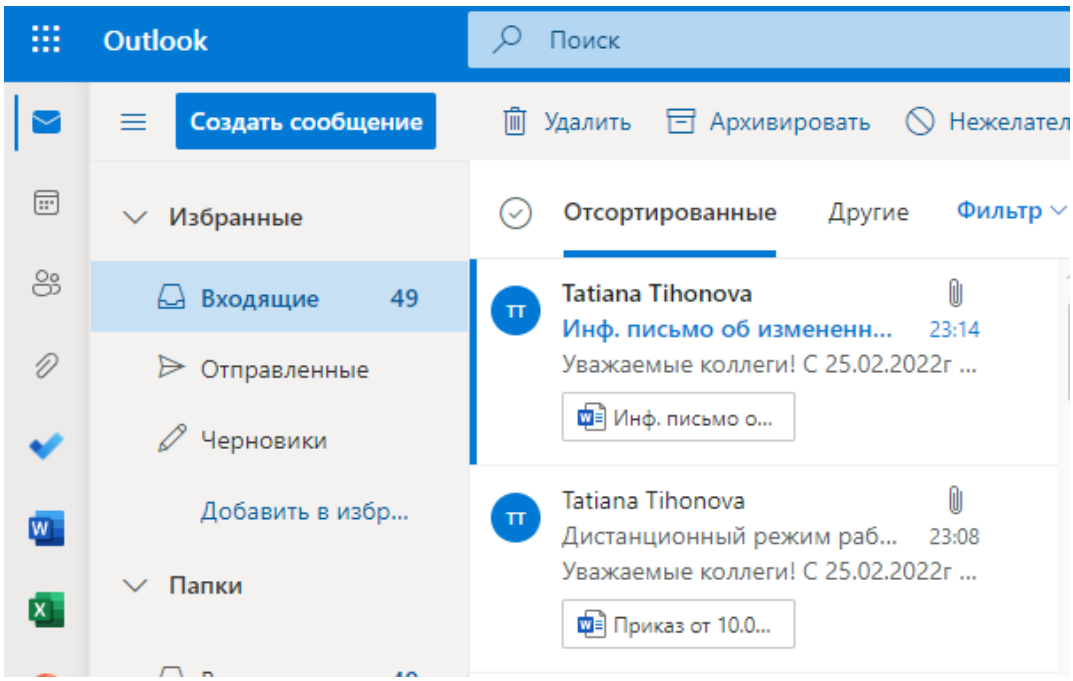
Увы, встраивание ссылки в текст приводи к залету в спам ☹

* Уворачиваемся от спама*

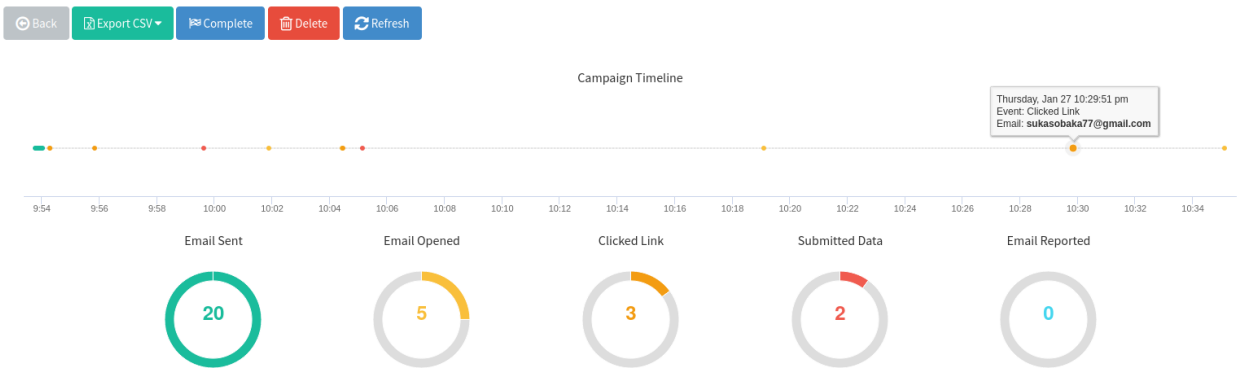
Итак, вооружившись всем необходимым, открываем любимый напиток и смотрим рыбов.



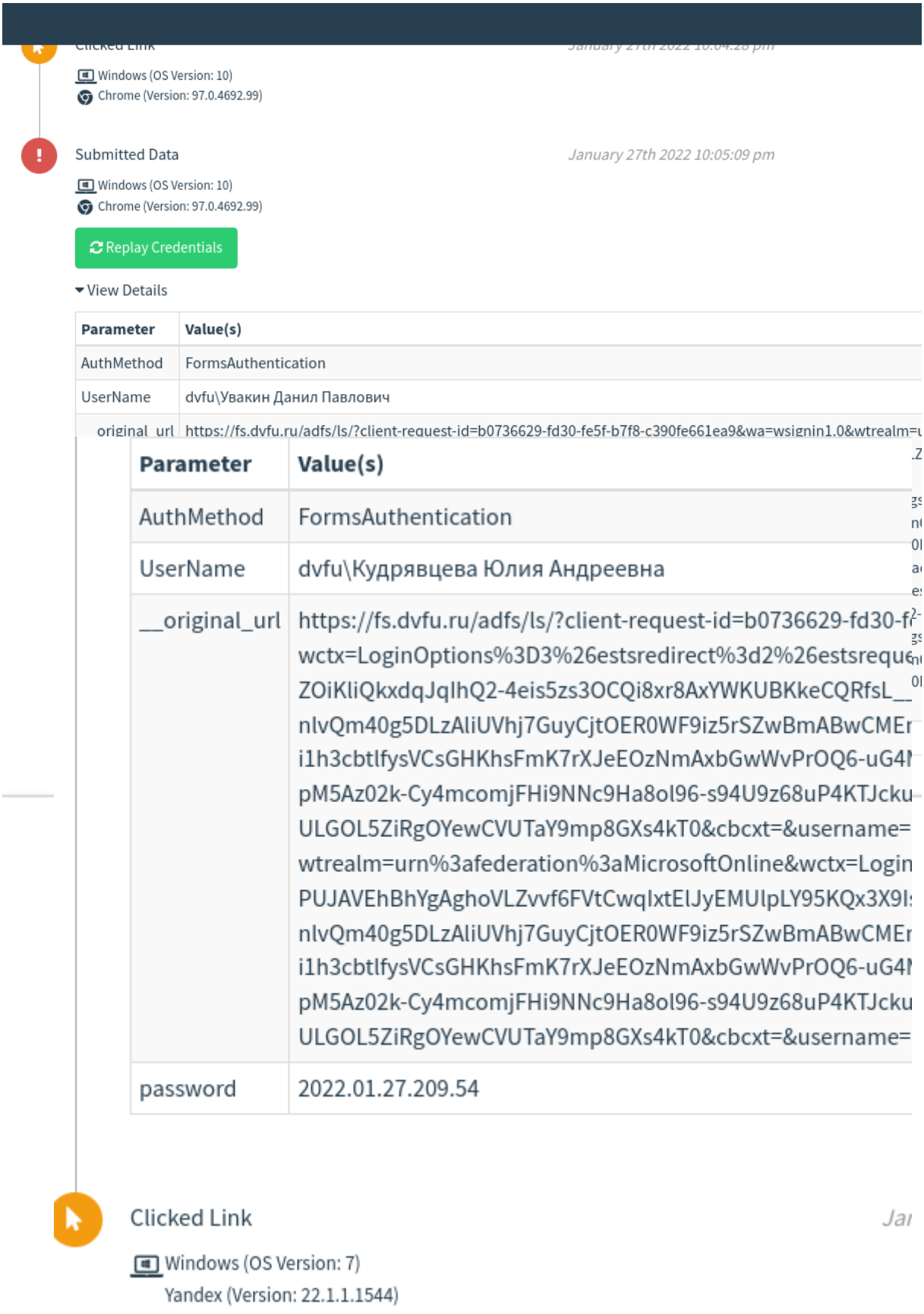




Results for Copy of DVFU



Details


Windows (OS Version: 10)
Chrome (Version: 97.0.4692.99)
Submitted Data
January 27th 2022 10:05:09 pm
Windows (OS Version: 10)
Chrome (Version: 97.0.4692.99)
Replay Credentials
View Details
Parameter
Value(s)
AuthMethod
FormsAuthentication
UserName
dvfu\Увакин Данил Павлович
original_url
https://fs.dvfu.ru/adfs/ls/?client-request-id=b0736629-fd30-fe5f-b7f8-c390fe661ea9&wa=wsignin1.0&wtrealm=u
Parameter
Value(s)
AuthMethod
FormsAuthentication
UserName
dvfu\Кудрявцева Юлия Андреевна
__original_url
https://fs.dvfu.ru/adfs/ls/?client-request-id=b0736629-fd30-f
wctx=LoginOptions%3D3%26estsredirect%3d2%26estsreque
ZOiKliQkxdqJqlhQ2-4eis5zs3OCQi8xr8AxYWKUBKkeCQRfsL__
nlvQm40g5DLzAliUVhj7GuyCjtOER0WF9iz5rSZwBmABwCMEr
i1h3cbtlfysVCsGHKhsFmK7rXJeEOzNmAxbGwWvPrOQ6-uG4
pM5Az02k-Cy4mcomjFHi9NNc9Ha8ol96-s94U9z68uP4KTJcku
ULGOL5ZiRgOYewCVUTaY9mp8GXs4kT0&cbcxt=&username=
wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=Login
PUJAVEhBhYgAghoVLZvvf6FVtCwqIxtElJyEMUlpLY95KQx3X9I
nlvQm40g5DLzAliUVhj7GuyCjtOER0WF9iz5rSZwBmABwCMEr
i1h3cbtlfysVCsGHKhsFmK7rXJeEOzNmAxbGwWvPrOQ6-uG4
pM5Az02k-Cy4mcomjFHi9NNc9Ha8ol96-s94U9z68uP4KTJcku
ULGOL5ZiRgOYewCVUTaY9mp8GXs4kT0&cbcxt=&username=
password
2022.01.27.209.54
Clicked Link
Windows (OS Version: 7)
Yandex (Version: 22.1.1.1544)

Также результаты от нашего шпиона:

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 77.34.185.218.

Basic Details:

Channel	HTTP
Time	2022-01-27 13:12:41 (UTC)
Canarytoken	gclyhgtq3ecr5qra1x7ratc1k
Token Reminder	Laba 2
Token Type	ms_word
Source IP	77.34.185.218
User Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; Zoom 3.6.0; ms-office; MSOffice 16)

An HTTP Canarytoken has been triggered by the Source IP 217.150.73.171.

Basic Details:

Channel	HTTP
Time	2022-01-27 13:17:34 (UTC)
Canarytoken	jqsj82eqiign31pehtctfojji
Token Reminder	LAB TWO
Token Type	ms_word
Source IP	217.150.73.171
User Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Tablet PC 2.0; Zoom 3.6.0; ms-office; MSOffice 16)

Итог: С Gophish подружились, письма отправили, пароли получили, спам обошли.

Теперь мы знаем как замучить своих подчиненных спамом, доказать, что они клюнули на фишинг, а потом наказать ☺. ..и стырить пароли ☺