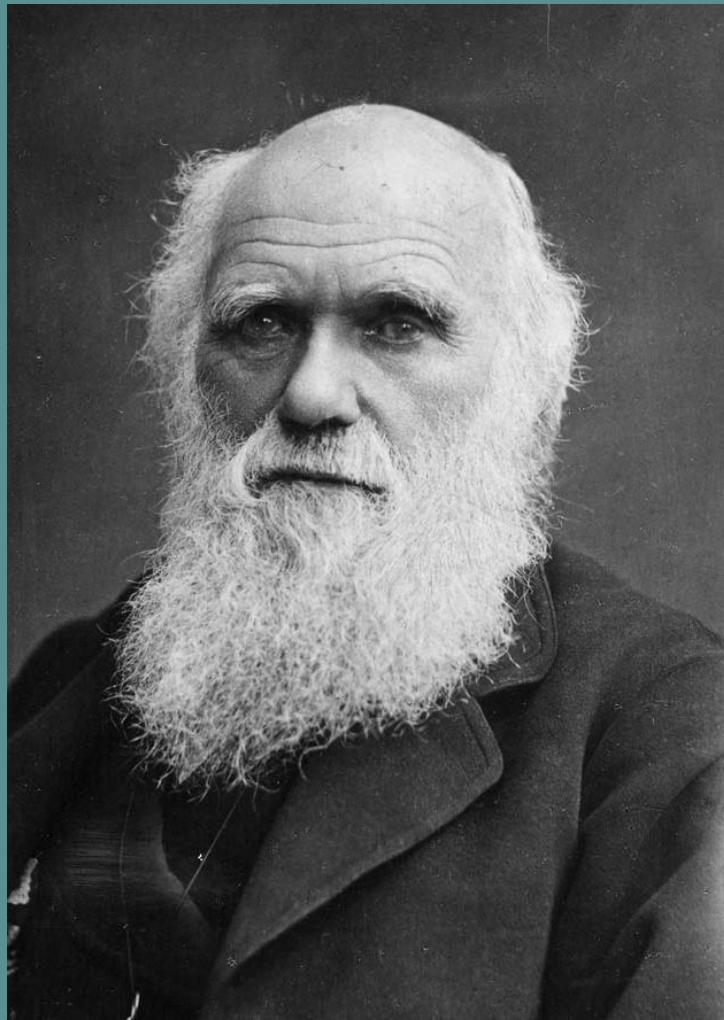


TALES FROM THE CRYPT

ABOUT PHISHING

by Arthur Hil



What is phishing?

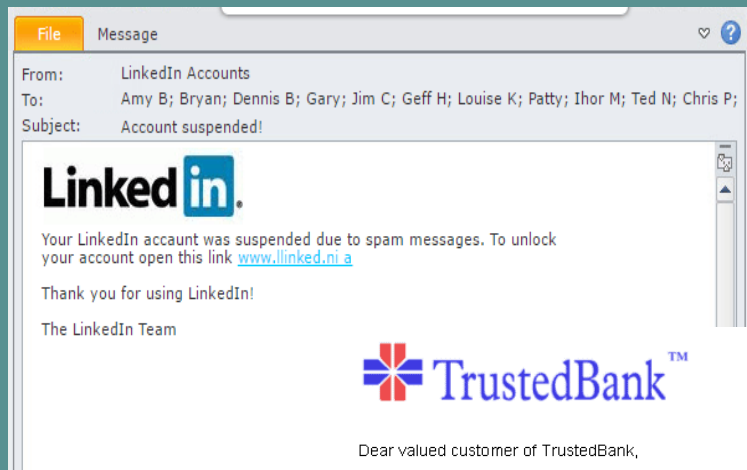


- Email
- Bank info
- Files
- Malware
- Ransomware
- Money
- etc...

<https://en.wikipedia.org/wiki/Phishing>

<http://www.phishing.org/what-is-phishing>

Email phishing



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

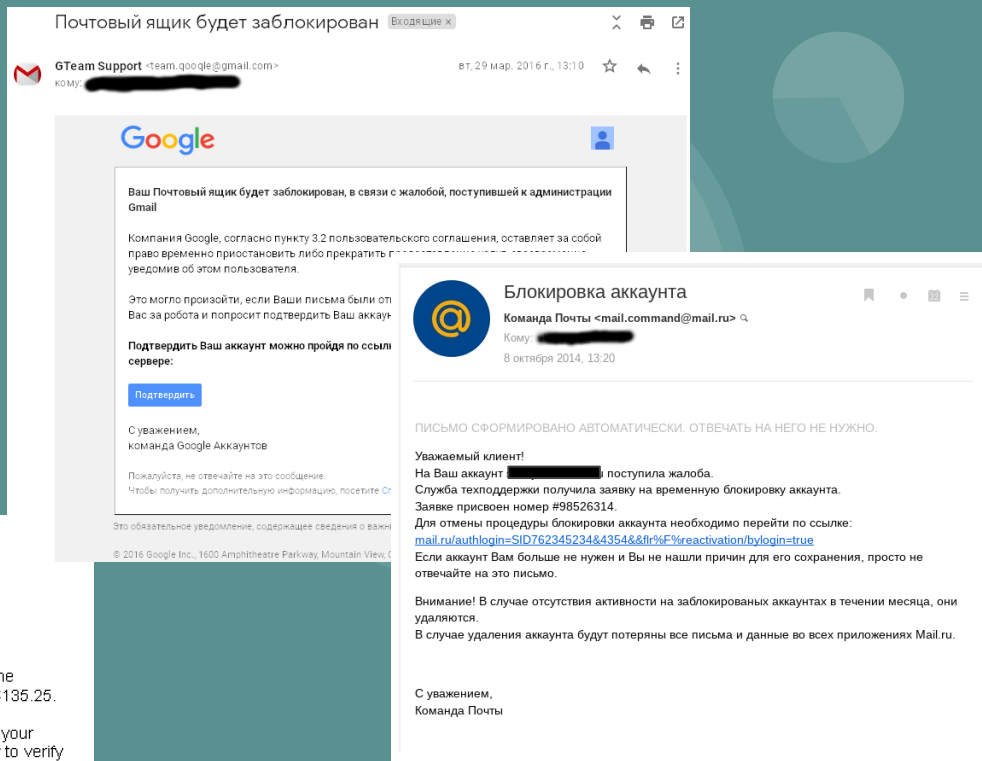
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

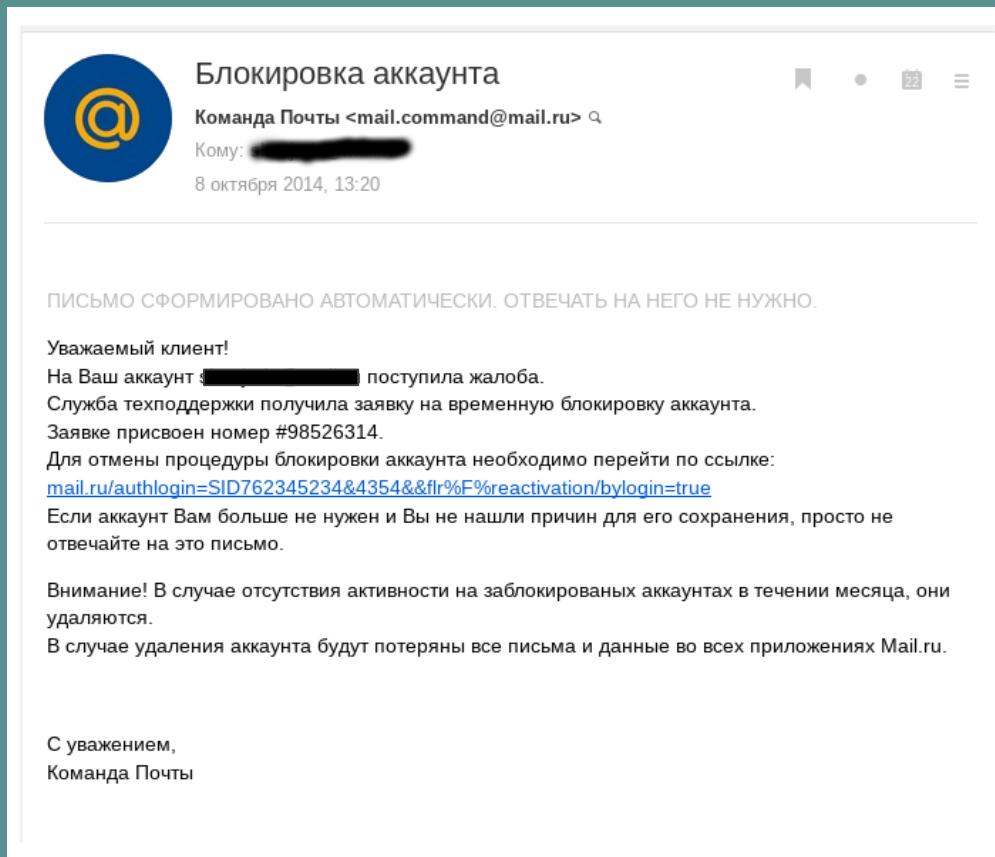
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.




Triggers





- Interesting title
- Avatar
- From:
- Text

Make your choice

Почтовый ящик будет заблокирован Входящие x

У  **GTeam Support** <team.google@gmail.com> вт, 29 мар. 2016 г., 13:10
кому: [REDACTED]

Ваш Почтовый ящик будет заблокирован, в связи с жалобой, поступившей к администрации Gmail

Компания Google, согласно пункту 3.2 пользовательского соглашения, оставляет за собой право временно приостановить либо прекратить предоставление услуг, своевременно уведомив об этом пользователя.

Это могло произойти, если Ваши письма были отмечены опцией «спам» - система приняла Вас за робота и попросит подтвердить Ваш аккаунт.

Подтвердить Ваш аккаунт можно пройдя по ссылке и дополнительно авторизовавшись на сервере:

[Подтвердить](#)

С уважением,
команда Google Аккаунтов

Пожалуйста, не отвечайте на это сообщение.
Чтобы получить дополнительную информацию, посетите [Справочный центр Google Аккаунтов](#).

Это обязательное уведомление, содержащее сведения о важных изменениях в Вашем аккаунте.

© 2016 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

We need more html!

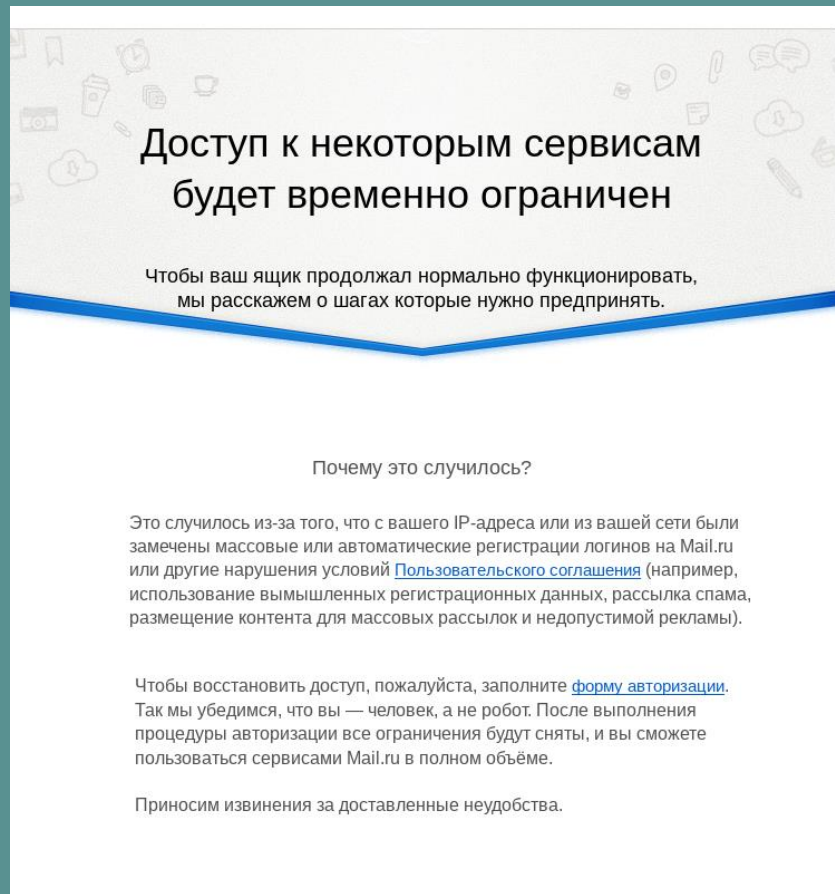
More css

More images

More logos

More official terms

`http://34.45.74.12/mail.ru/settings/security/login2.php?id=cXdlcnR5QG1haWwucnU=`



**Доступ к некоторым сервисам
будет временно ограничен**

Чтобы ваш ящик продолжал нормально функционировать,
мы расскажем о шагах которые нужно предпринять.

Почему это случилось?

Это случилось из-за того, что с вашего IP-адреса или из вашей сети были замечены массовые или автоматические регистрации логинов на Mail.ru или другие нарушения условий [Пользовательского соглашения](#) (например, использование вымышленных регистрационных данных, рассылка спама, размещение контента для массовых рассылок и недопустимой рекламы).

Чтобы восстановить доступ, пожалуйста, заполните [форму авторизации](#). Так мы убедимся, что вы — человек, а не робот. После выполнения процедуры авторизации все ограничения будут сняты, и вы сможете пользоваться сервисами Mail.ru в полном объеме.

Приносим извинения за доставленные неудобства.

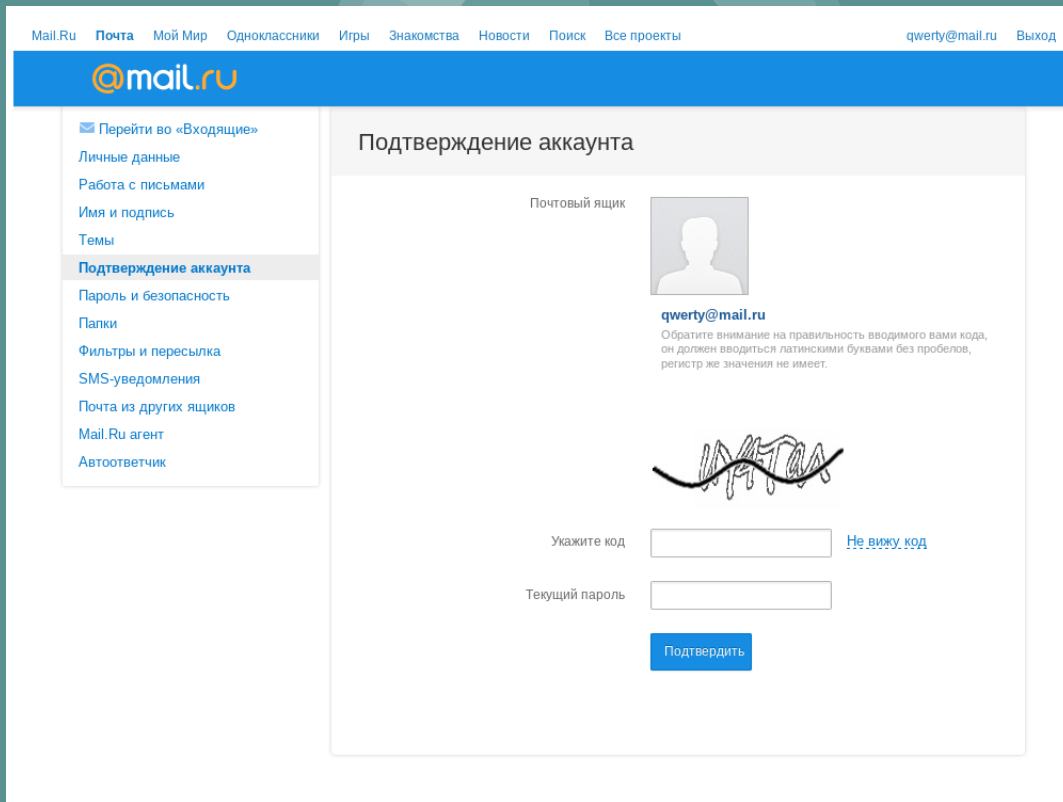
How deep the rabbit hole goes or what is on the dark side?

cXdIcnR5QG1haWwucnU=

base64



qwerty@mail.ru



Where is your domain, dude?

www.xn--oole-9pb06e.com.

-->

www.google.com.

ww25.xn--gogle-uob.com.

-->

ww25.google.com.

xn--ggle-lqaa.com.

-->

gòogle.com.

xn--gogl-1nd42e.com.

-->

google.com.

xn--gogle-7ta.com.

-->

goôgle.com.

xn--gogle-jua.com.

-->

göogle.com.

xn--gogle-kua.com.

-->

goögle.com.

xn--gogle-uta.com.

-->

gòogle.com.

xn--gogle-vob.com.

-->

gooogle.com.

xn--googl-n0a.com.

-->

google.com.

xn--oogl-epa71n.com.

-->

googlé.com.

xn--oogle-v1a.xyz.

-->

google.xyz.

Dive deeper



- +Don't block by google
- +Trusted Google SSL cert.
- +Real Google domain
- Can't store data

- +Can store data
- +Easy to link
- +Easy to access

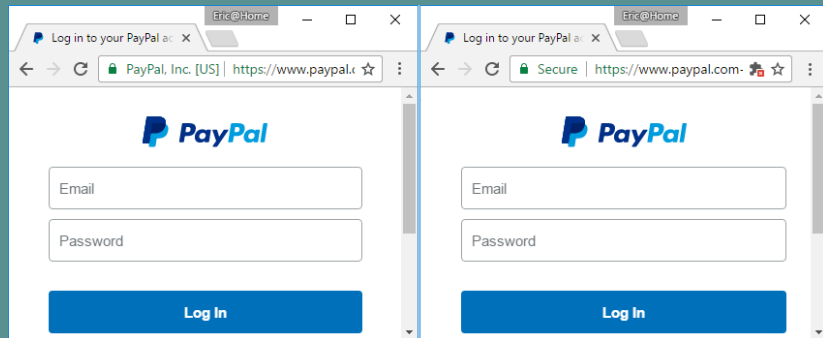
Not all "S" are equally useful.

HTTP

http://domain-name.com

HTTPS

Secure | https://domain.com



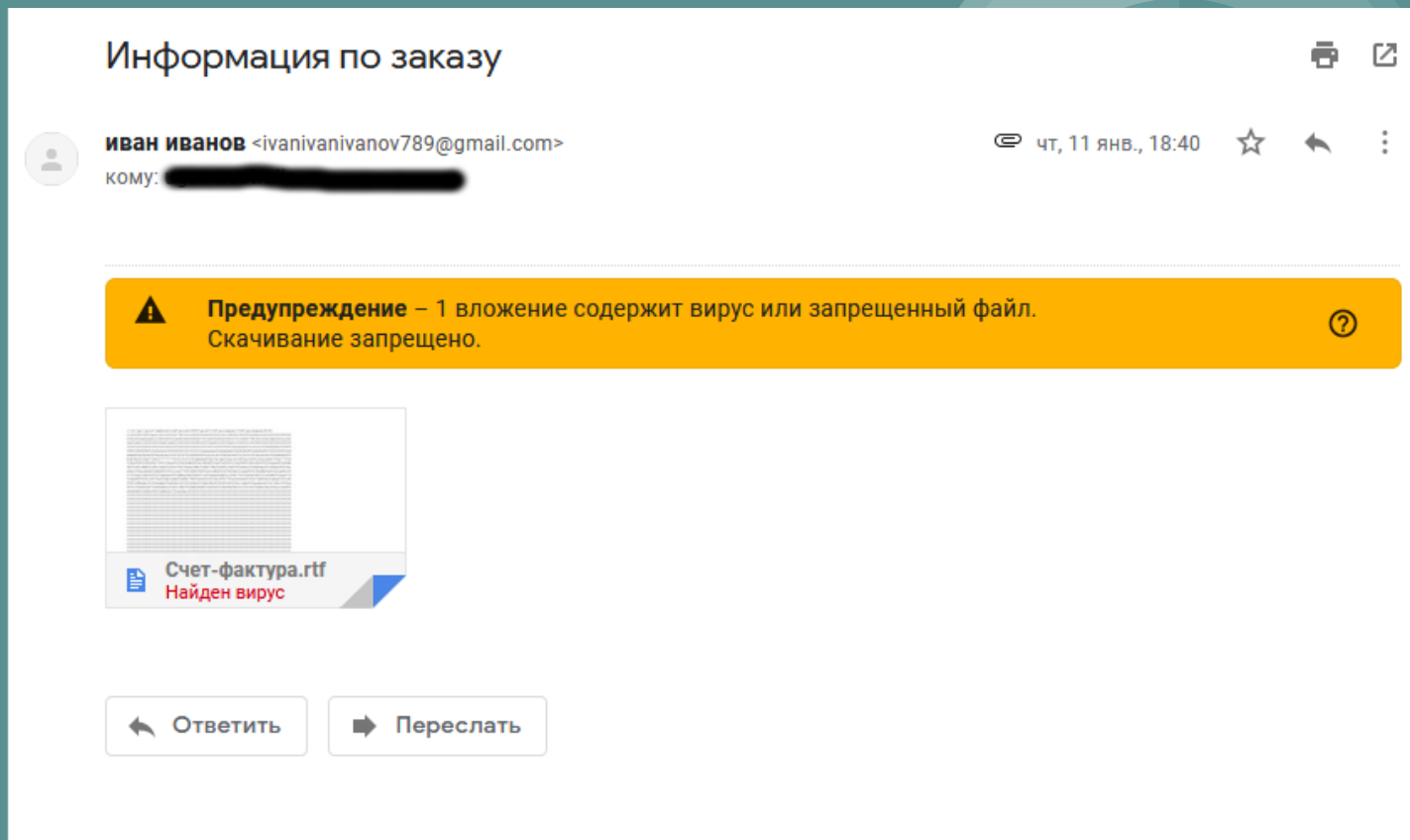
One real, one fake, your account is at stake.

Month	# of Certs Issued
March 2016	10
April 2016	57
May 2016	73
June 2016	65
July 2016	149
August 2016	231
September 2016	299
October 2016	536
November 2016	1276
December 2016	2530
January 2017	3995
February 2017	5101

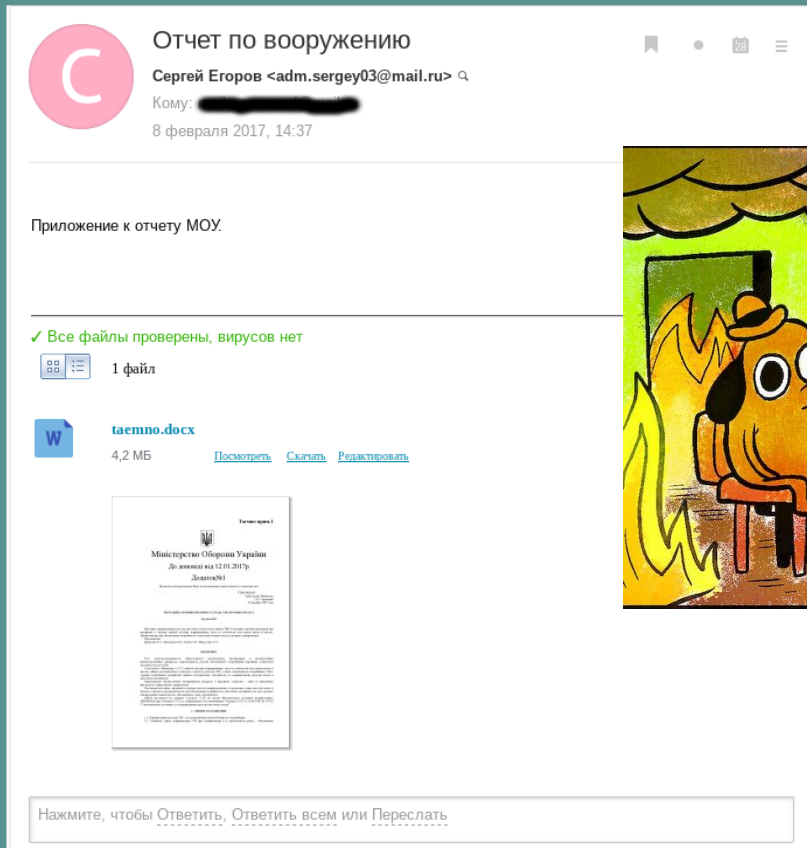
What inside the mailbox?



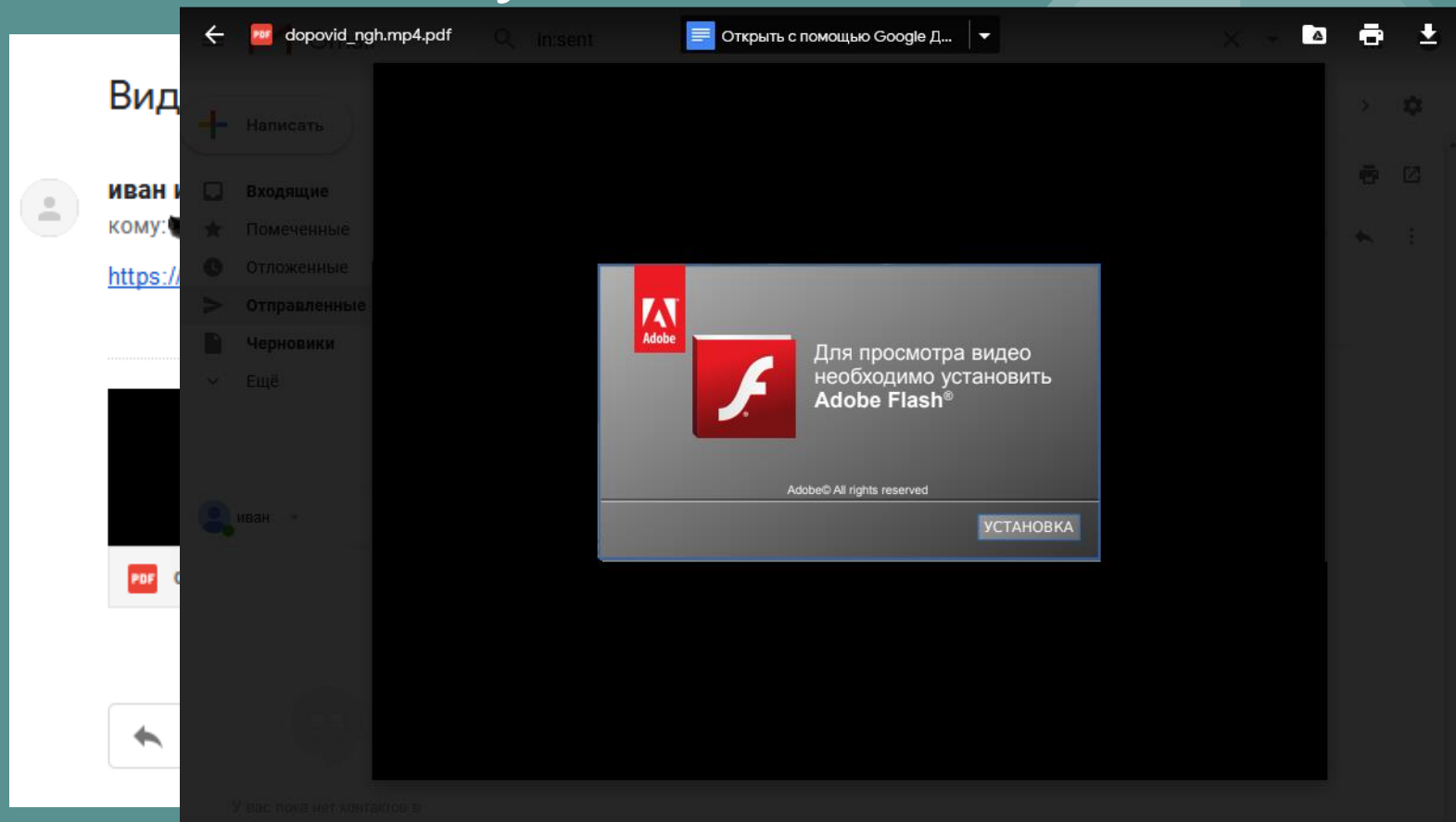
Google is watching



Old good buddy HTML+Base64



Another way



**How to be
informed and
ready?**



That's all folks

