ПРИМЕРИ МАЛИЦИОЗНИХ МЕЈЛОВА

1) Већ су постали уобичајени покушаји "пецања" на тему попуњености мејл налога и његовог скорог гашења где се од корисника тражи да се логује пореко понуђеног линка и на тај начин спречи губитак свог налога електронске поште. Пример једног таквог мејла:

Subject: vet.bg.ac.rs Email Service DE-activation FINAL WARNING ALERT
Date: 2020-09-01 02:21
From: vet.bg.ac.rs Admin <sales@wecquerybulk.info>
To: korisnicko.ime@vet.bg.ac.rs

EMAIL UPDATE vet.bg.ac.rs

Dear korisnicko.ime@vet.bg.ac.rs

You will be deactivated from using this service Because you

failed to upgrade your mail.

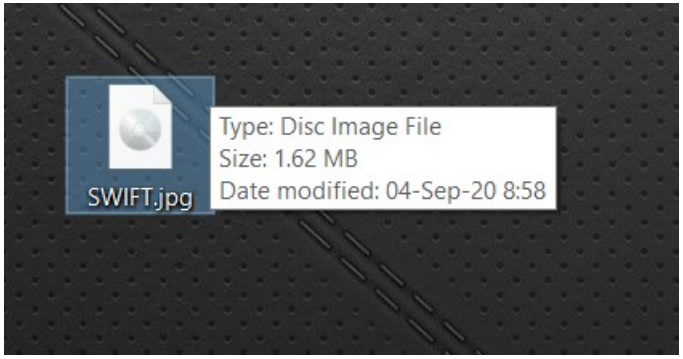
To avoid account shutdown
CLICK HERE TO VERIFY NOW [1]

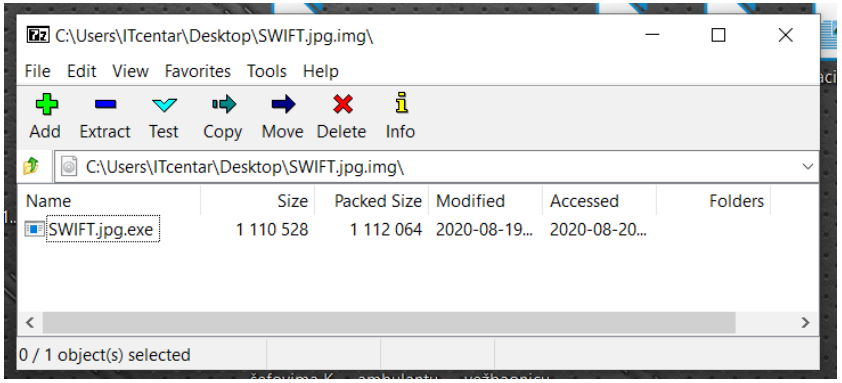
Admin Team vet.bg.ac.rs

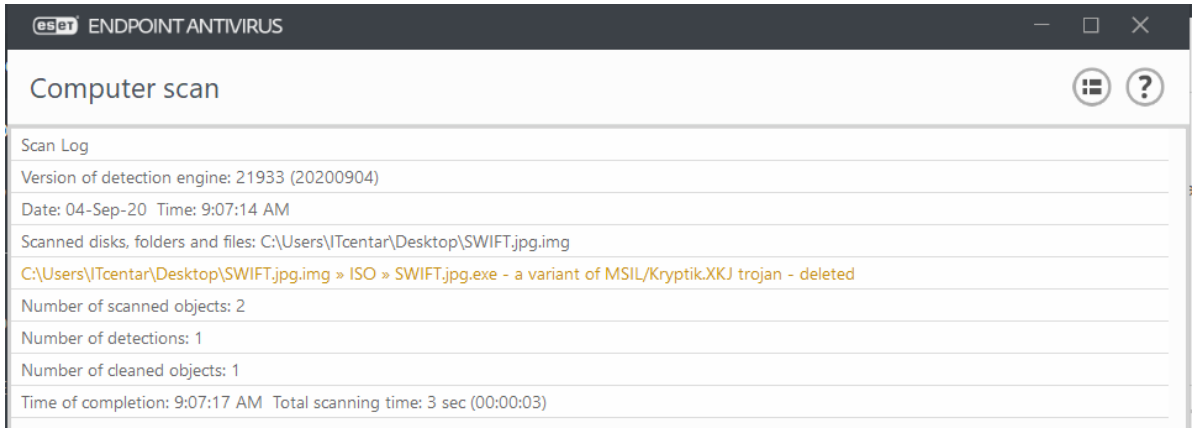
Подсећамо Вас да нико и никада нема разлог и право да тражи корисничко име и лозинку за Ваш мејл налог, као и да исте уносите искључиво путем *webmail* форме (на званичној страни факултета) или наменских емаил програма на свом рачунару (*Outlook*, *Thunderbird*, итд.), а никако преко линкова које Вам понуде у мејловима!

2) Све су чешћи и случајеви где се у прилогу мејлова налазе малициозни фајлови који су именовани тако да просечан корисник на *Windows* рачунару не уочи њихову праву природу. Примери оваквих мејлова су наводне поруке од банке о новцу који се уплаћује или рефундира на Ваш рачун, где је у прилогу потврда о уплати коју се очекује да преузмете и отворите на свом рачунару. Нпр. фајл SWIFT.jpg.img ће се на *Windows* рачунару са подразумеваним подешавањима приказати само као SWIFT.jpg што корисника може навести да помисли да је у питању слика у JPEG формату коју је безбедно отворити, а уствари је у питању .img слика диска која се поготово на *Windows 10* рачунарима лако "монтира" (*mount*) путем двоклика и систем га надаље види као додатни CD/DVD уређај подложан *Auto-play* функцији која аутоматски покреће садржај диска - што је најчешће "тројанац" чији је задатак да даље преузме и инсталира друге злонамерне програме за крађу или закључавање података на рачунару.

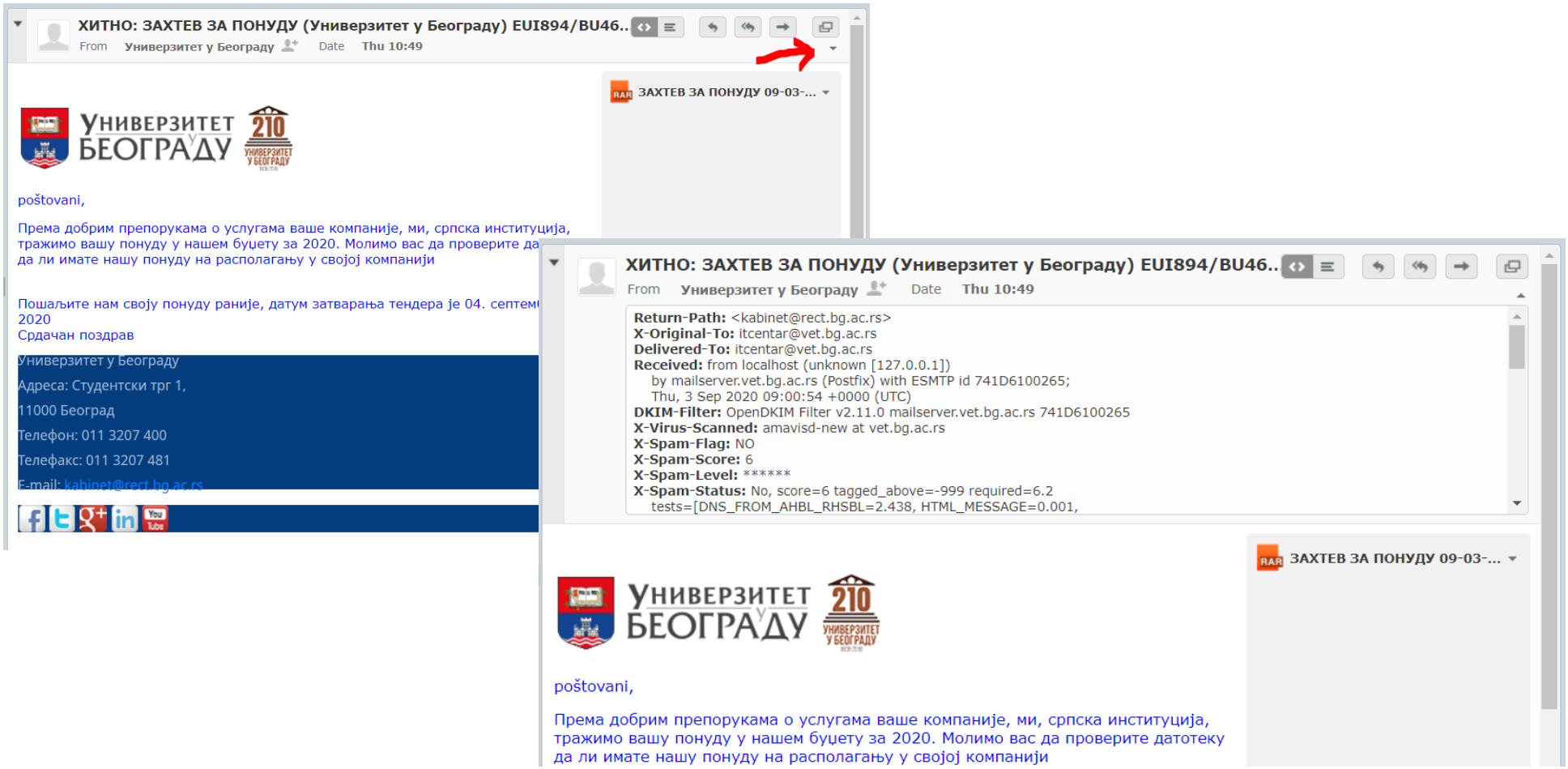
На сликама се види поменути фајл преузет на десктоп, затим отворен у 7zip програму као архива да би се приказао његов садржај (без покретања), и на крају резултат скенирања фајла ECET антивирусом (што препоручујемо да ручно урадите са сваким сумњивим фајлом који преузмете на свој рачунар).





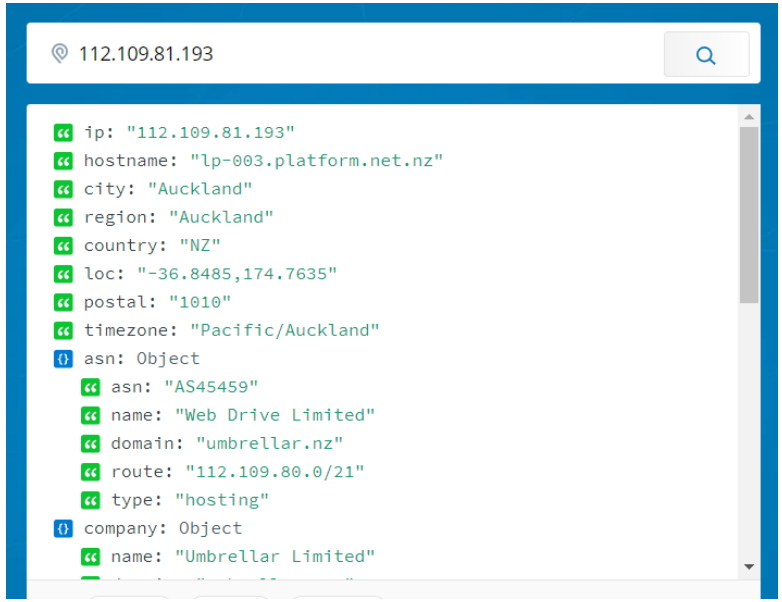


3) Поље у заглављу мејла у којем се приказује (наводни) пошиљалац је лако маскирати, па ако Вам садржај самог мејла делује чудно, пожељно је да проверите да ли је мејл заиста стигао са наведене адресе. То се може видети отварањем изворног заглавља поруке (опција се најчешће зове *View source* или *Show headers*). У примеру на сликама (са *webmail*-а) имамо поруку наводно пристиглу из кабинета Ректората Универзитета у Београду (неко се заиста потрудио да постави праве линкове ка презентацијама Универзитета на друштвеним мрежама), чији невешти текст сугерише да је у питању машински преведени текст на српски језик путем *Google Translate*-а или неке сличне опције. Уколико кликнемо на стрелицу у горњем десном углу приказаће нам се изворно заглавље поруке.



У садржају заглавља обратите пажњу на поља *Received*: и евентуално *Authentication-Results* ако постоји:

```
Return-Path: <kabinet@rect.bg.ac.rs>
X-Original-To: itcentar@vet.bg.ac.rs
Delivered-To: itcentar@vet.bg.ac.rs
Received: from localhost (unknown [127.0.0.1])
        by mailserver.vet.bg.ac.rs (Postfix) with ESMTP id 741D6100265;
        Thu,  3 Sep 2020 09:00:54 +0000 (UTC)
DKIM-Filter: OpenDKIM Filter v2.11.0 mailserver.vet.bg.ac.rs 741D6100265
X-Virus-Scanned: amavisd-new at vet.bg.ac.rs
X-Spam-Flag: NO
X-Spam-Score: 6
X-Spam-Level: ******
X-Spam-Status: No, score=6 tagged_above=-999 required=6.2
        tests=[DNS_FROM_AHBL_RHSBL=2.438, HTML_MESSAGE=0.001,
        RCVD_IN_RP_RNBL=1.284, SPF_NEUTRAL=0.652, SUBJ_ALL_CAPS=1.625]
        autolearn=disabled
Received: from mailserver.vet.bg.ac.rs ([127.0.0.1])
        by localhost (mailserver.vet.bg.ac.rs [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id 7p8Hd2CQ79a0; Thu,  3 Sep 2020 11:00:51 +0200 (CEST)
X-Greylist: delayed 605 seconds by postgrey-1.34 at mailserver.vet.bg.ac.rs; Thu, 03 Sep
2020 11:00:48 CEST
DMARC-Filter: OpenDMARC Filter v1.3.2 mailserver.vet.bg.ac.rs 829791002C6
DKIM-Filter: OpenDKIM Filter v2.11.0 mailserver.vet.bg.ac.rs 829791002C6
Received: from lp-003.platform.net.nz (lp-003.platform.net.nz [112.109.81.193])
        (using TLSv1.2 with cipher ADH-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by mailserver.vet.bg.ac.rs (Postfix) with ESMTPS id 829791002C6;
        Thu,  3 Sep 2020 11:00:48 +0200 (CEST)
Received: from webmail.16management.com (localhost [IPv6:::1])
        by lp-003.platform.net.nz (Postfix) with ESMTPSA id F06621D38E1;
        Thu,  3 Sep 2020 20:49:58 +1200 (NZST)
Authentication-Results: lp-003.platform.net.nz;
        spf=pass (sender IP is ::1) smtp.mailfrom=kabinet@rect.bg.ac.rs smtp.helo=webmail.16management.com
Received-SPF: pass (lp-003.platform.net.nz: connection is authenticated)
MIME-Version: 1.0
```



Прва два поља (означено зеленом бојом) у којима се спомиње mailserver.vet.bg.ac.rs значе само да је *webmail* или програм у којем прегледате пошту преузео поруку са нашег сервера. Друга два поља означена црвеном бојом показују да је пошта оригинално примљена са **platform.net.nz** домена који припада Новом Зеланду, што се може проверити и уносом ИП адресе 112.109.81.193 на неком сајту попут https://ipinfo.io/ (на слици изнад). Самим тим можемо закључити да порука није послата из Кабинета Ректората и да би је требало игнорисати/обрисати. Додатно, приложени фајл је именован слично као онај у тачки 2) са циљем да превари корисника да помисли да је у питању .pdf фајл и отвори прилог (који је уствари .rar архива са малициозним извршним фајлом):