

УПУТСТВО ЗА ПАЖЉИВО ЧИТАЊЕ МЕЈЛОВА - ЗАШТИТА ОД ПЕЦАЊА (PHISHING) -

Садржај:

1. Пошиљалац можда није прави	4
2. Приказивање имејл адресе пошиљаоца.....	6
3. Чувајте се прилога у е-писмима.....	8
4. Читајте “Headers” (заглавље) е-писма.....	10
5. Уочите структуру исправног е-писма од администратора веб-сервера.....	12
6. Провера малициозности Веб сајта чија посета Вам је предложена у фишинг е-поруци	13
7. Како да сами препознате малициозни сајт	15

Пецање (енгл. *phishing*) је врста интернет преваре где нападач помоћу е-писма покушава да украде Ваше креденцијале (корисничко име и лозинка) или да зарази Ваш рачунар. Оваква електронска пошта је све чешћа и функционише тако што се хакери тј. сајбер криминалци представљају као велике компаније попут банака, удружења или ИТ гиганата, а све чешће и као институције (Универзитет у Београду, факултети Универзитета у Нишу и Крагујевцу, па и наш матични факултет) и наводе вас да преузмете и отворите фајлове који се налазе у прилогу или кликнете на линк који се налази у поруци како би дошли до Ваших личних информација. Израз „*phishing*“ је настао од енглеске речи за пецање пошто хакери оваквом поштом „*бацају удицу*“ као у пецању и чекају да се неко од циљаних корисника „*упеца*“.

У наставку је изложено кратко упутство, листа савета, како да правилно и пажљиво читате мејлове и оцените оне који су сумњиви. Сви снимци екрана су аутентични - то су мејлови које су примали наши наставници и запослени у администрацији и који представљају примере „*пецања*“.

Ма колико тежили да ово упутство уопшtimo, увек ће постојати случај који није покривен овим саветима. Тада је најсигурније писати на адресу admin@matf.bg.ac.rs и проследити мејл за који нисте сигурни да је исправан.

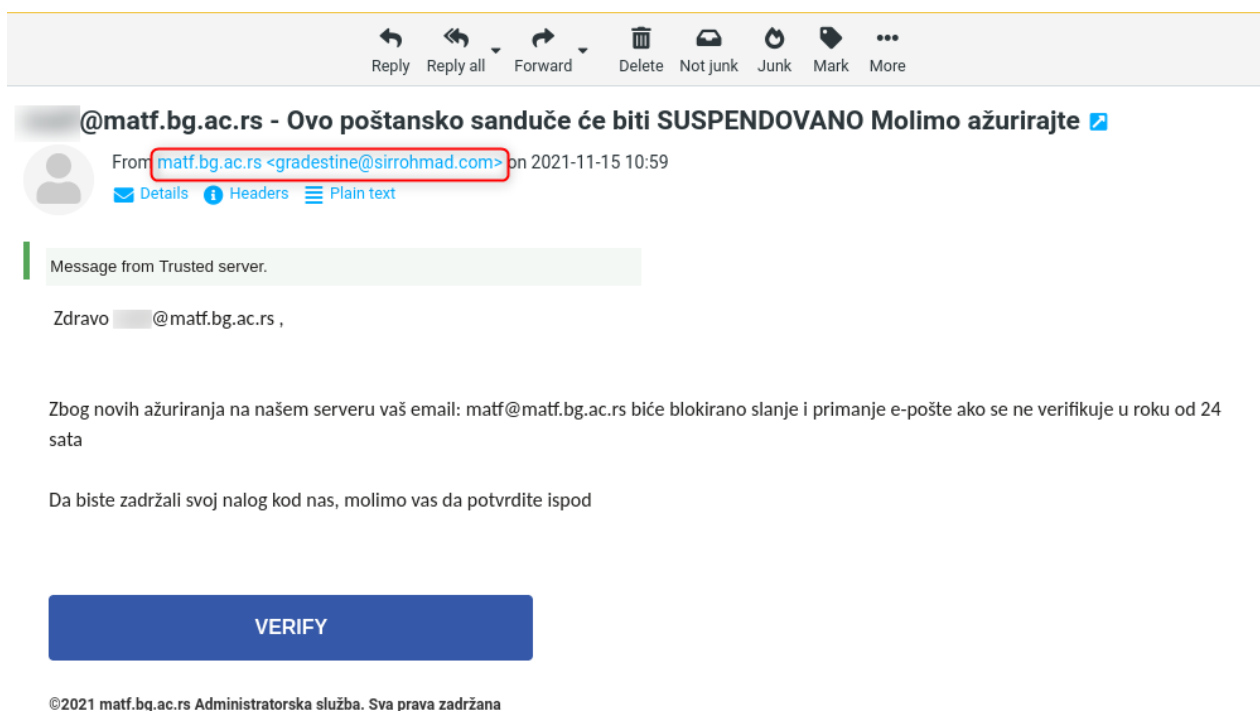
Хвала што чувате Ваш и наш сервер од злонамерних напада!



1. Пошиљалац можда није прави

У пољу “Од” (“From”) може бити лажна информација. Уобичајена је пракса да се у пољу где пише име пошиљача упише мејл адреса која се веома мало разликује од легитимне адресе која Вам може бити позната.

На слици ниже приказан је мејл који је примљен од пошиљача “matf.bg.ac.rs”, користећи непознату мејл адресу.



Ово е-писмо има још делова који га јасно одају као непожељну и злонамерну поруку: обраћање кориснику по његовој е-адреси, а не имену, поруку да ће ускоро доћи до брисања налога, дугме “Verify” и друго.

На наредној слици приказана је слична ситуација. Пошиљалац је “Admin” који опет користи непознату адресу, а у поруци обавештава да ће доћи до брисања корисничког налога и да треба кликнути на линк (који поново није ни на који начин повезан са нашим матичним сајтом или неким од сервера Математичког факултета).

Reply Reply all Forward Delete Not junk Junk Mark More

KONAČNO OBAVEŠTENJE/UPOZORENJE



From: Admin <jezik@tmn.sk> on 2021-10-27 08:58

Details Headers

Poštovani korisniče (KRAJNJE OBAVEŠTENJE/UPOZORENJE):

vršimo godišnje ažuriranje i održavanje veb-pošte, brišemo sve nekorišćene naloge e-pošte da bismo napravili mesta za aktivan i funkcionalan nalog e-pošte. Preporučuje se da pregledate svoj nalog za veb poštu kako ne bi bio izbrisan kao neiskorišćen nalog. Da biste ažurirali svoj nalog e-pošte, kliknite ovde ILI kopirajte vezu ispod.

<http://webadminn.moonfruit.com>



--

This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

Још пар примера са шаблоном за “пецање”.

Reply Reply all Forward Delete Not junk Junk Mark More

matf@matf.bg.ac.rs Update Your Account With matf.bg.ac.rs



From: Email Account Update <update2021@cnmetaldetector.com> on 2021-11-22 00:16

Details Headers Plain text

Hello ,

Kindly Update your email account with

domain matf.bg.ac.rs before it will be blocked

[CLICK HERE TO UPDATE](#)

Note: This is a general upgrade to everyone using our ei

Email Update 2021

matf.bg.ac.rs Servers 2021

11/21/2021 3:16:47 p.m.

Six Incoming messages are on hold



From: matf.bg.ac.rs <dscott@gtrebol.com> on 2021-11-18 01:32

Details Headers Plain text

From matf.bg.ac.rs Server Admin

Six messages are still waiting to be delivered to your inbox since Nov 08th, 2021.

Mailbox:matf@matf.bg.ac.rs

Subject	Recipient	Date
FW: Invoice copy AWB No. 325-2322	To: matf@matf.bg.ac.rs	12/11/2021
Updated Sea Freight Quotation	To: matf@matf.bg.ac.rs	12/11/2021
AW: PO#203477 INVOICES	To:matf@matf.bg.ac.rs	12/11/2021
Re: Regarding the preparation of the 06/0/2021 plan by the start-up department	To: matf@matf.bg.ac.rs	10/11/2021
Fwd: Payment ---- Forwarded message ----	To: matf@matf.bg.ac.rs	10/11/2021
COVID-19 Safety Measures	To: matf@matf.bg.ac.rs	08/11/2021

1. [Release Pending Mails to inbox](#)

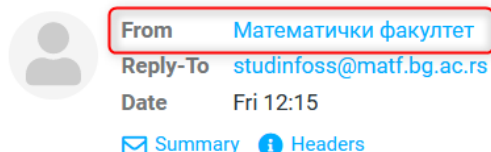
2. [Report Error To IT Help Desk](#)

You will receive pending emails after successful login via portal as we apologize for the inconvenience.

2. Приказивање имејл адресе пошиљаоца

Подразумевано подешавање у вебмејлу Roundcube је да у пољу „Од“ („From“) не приказује мејл пошиљаоца, него само име, као на следећој слици:

Откривена је сумњива активност на вашем налогу



--

Корисник се управо пријавио на ваш налог са новог уређаја ипхоне 12 про мак. шаљемо вам ову е-пошту да потврдимо да сте то заиста ви. Морате одмах да промените своју лозинку. Молимо вас да се пријавите помоћу нашег безбедног портала као што је приказано испод и промените лозинку.

<https://bit.ly/3TAplB1>

=====

Рачунарска лабораторија

Математички факултет

--

Тада је потребно да:

- Settings (1)
- Preferences (2)
- Displaying Messages (3)
- активирате Show email address with display name (4)
- и за крај клинете Save (5)

The screenshot shows the Outlook 'Settings' window. The left sidebar has 'Settings' highlighted (1). The top bar has 'Preferences' (2). The left pane has 'Displaying Messages' selected (3). The 'Main Options' section has 'Show email address with display name' toggle turned on (4). The 'Save' button is at the bottom (5).

Након тога ће Вам у пољу „Од“ бити приказани и име пошиљаоца и мејл адреса са које је послата порука.

Откривена је сумњива активност на вашем налогу

From Математички факултет <studinfo@matf.bg.ac.rs>
Reply-To studinfo@matf.bg.ac.rs
Date Fri 12:15
[Summary](#) [Headers](#)

--

Корисник се управо пријавио на ваш налог са новог уређаја ипхоне 12 про макс. шаљемо вам ову е-пошту да потврдимо да сте то заиста ви. Морате одмах да промените своју лозинку. Молимо вас да се пријавите помоћу нашег безбедног портала као што је приказано испод и промените лозинку.

<https://bit.ly/3TAplB1>

=====

Рачунарска лабораторија

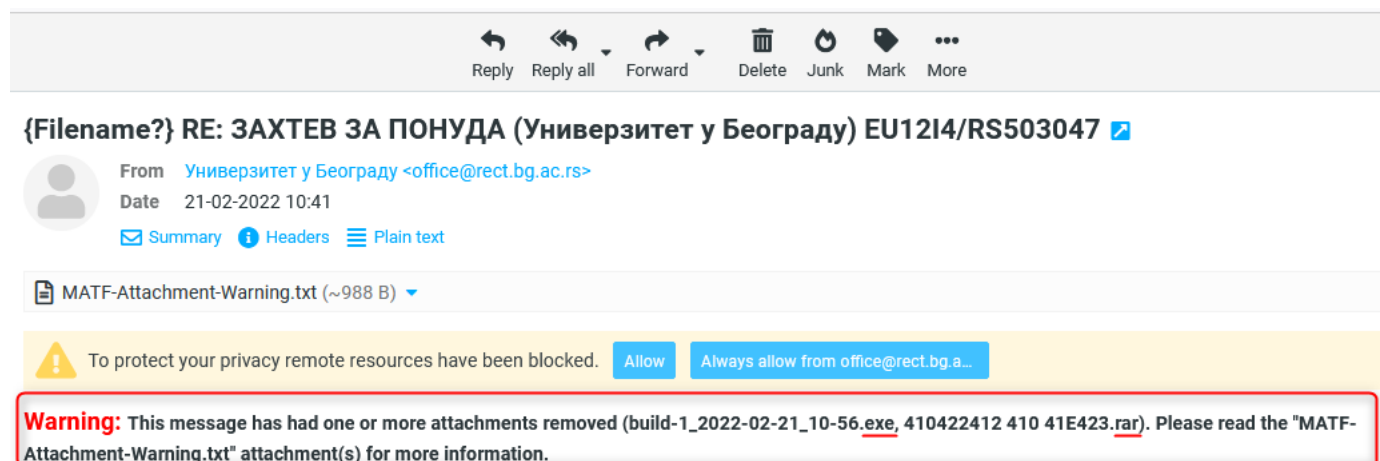
Математички факултет

3. Чувајте се прилога у е-писмима

Устаљени начин преваре у е-писмима је и подметање лажних прилога. **Најбољи и најсигурнији начин да избегнете злонамерни програм (малвер) је да прилоге из сумњивих е-писама никада не скидате и не отворате.** По правилу, не треба отворати никакав прилог ако је пошиљалац непознат, чак и када нема делова поруке који су описани у првом делу.

Прилог који је стигао у сумњивом мејлу често има непознати тип фајла (*формат, екстензију*) или чак двоструки формат, те можете добити прилог који има назив на пример - **zapisnikSaGlavneSednice.pdf.exe** чиме је покушана превара корисника. Документ је наизглед у познатом .pdf формату, али и поред тога на крају има ".exe" које означава да је реч о извршивом фајлу.

Следи пар аутентичних слика у којима су приказани примери овакве врсте преваре.



Здраво,

Према добрим препорукама о услугама Ваше компаније, ми, српска институција, тражимо Вашу понуду у нашем буџету за 2022. годину. Видите у прилогу
Пошаљите нам своју понуду раније, крајњи рок за тендер је 26.02.2022.
Хвала & Пуно поздрава

Универзитет у Београду
Адреса: Студентски трг 1,
11000 Београд
Телефон: 011 3207 400
Телефакс: 011 3207 481
Е-mail: kabinet@rect.bg.ac.rs

Слика изнад представља пример кривотвореног мејла који је написан ћирилицом, има грб Универзитета у Београду, а на крају се налази и листа прилога.

У наредном примеру дата је приближно иста ситуација, али наводни пошиљалац је други.

Као по правилу, ти прилози често садрже пун или скраћени назив наше установе као и неко обавештење или још чешће - упозорење (енгл. *Warning*).

{Filename?} Obaveštenje o deviznom prilivu za JBKJS 06395

From obavestjenja.devizno@trezor.gov.rs on 2022-03-09 11:54

Details Headers Plain text

MATF-Attachment-Warning.txt (~962 B)

{Filename?} Obaveštenje o deviznom prilivu za JBKJS 06395

From obavestjenja.devizno@trezor.gov.rs on 2022-03-09 11:54

Details Headers Plain text

Warning: This message has had one or more attachments removed (2Nalozi_202203.exe, Nalozi_2022030.zip). Please read the "MATF-Attachment-Warning.txt" attachment(s) for more information.

***Ово је...
...За сво...
...Поштом...

Warning: This message has had one or more attachments removed (2Nalozi_202203.exe, Nalozi_2022030.zip). Please read the "MATF-Attachment-Warning.txt" attachment(s) for more information.

У прилогу вам достављамо ОБАВЕШТЕЊЕ О ДЕВИЗНОМ ПРИЛИВУ.

У складу са чланом 38. став 2. Правилника о начину и поступку обављања платног промета у оквиру система консолидованог рачуна трезора за девизна средства („Службени гласник РС”, бр. 13/2017 и 51/2019), потребно је да истог или наредног дана од пријема овог обавештења доставите Вашој надлежној филијали Управе за трезор, код које имате отворен девизни подрачун, следећу документацију неопходну за правилно евидентирање прилива:

- оригинал писма (у два примерка) у којем се изјашњава да прихватају девизни прилив и наводе инструкцију за евидентирање и распоред девизног прилива (девизни износ, број девизног подрачуна на којем се евидентира девизни прилив и шифра основа наплате), као и референцу обавештења и НБС референцу обавештења. У случају конверзије девизног прилива на динарски подрачун, наводи се и број динарског подрачуна, девизни износ који се конвертује, шифра плаћања за динарски платни промет и опционо позив на број одобрења. Уколико се девизна средства конвертују на уплатни или евиденциони рачун, шифра плаћања и позив на број одобрења морају бити у складу са прописима који се прописује услови и начин вођења рачуна за уплату јавних прихода и распоред средстава са тих рачуна;
- обавештење о девизном приливу, које је у прилогу овог мејла.


Уколико не прихватају девизни прилив, потребно је да доставите оригинал писма (у два примерка) у којем се изјашњава да не прихватају девизни прилив и наводите разлог неприхватања прилива.

У случају потребе, Управа за трезор може тражити додатну документацију.

Уколико из објективних разлога нисте у могућности да доставите инструкције за евидентирање девизног прилива у горе наведеном року, потребно је да о томе писаним путем обавестите Вашу надлежну филијалу Управе за трезор.

С поштовањем,

Управа за трезор



УПРАВА ЗА ТРЕЗОР

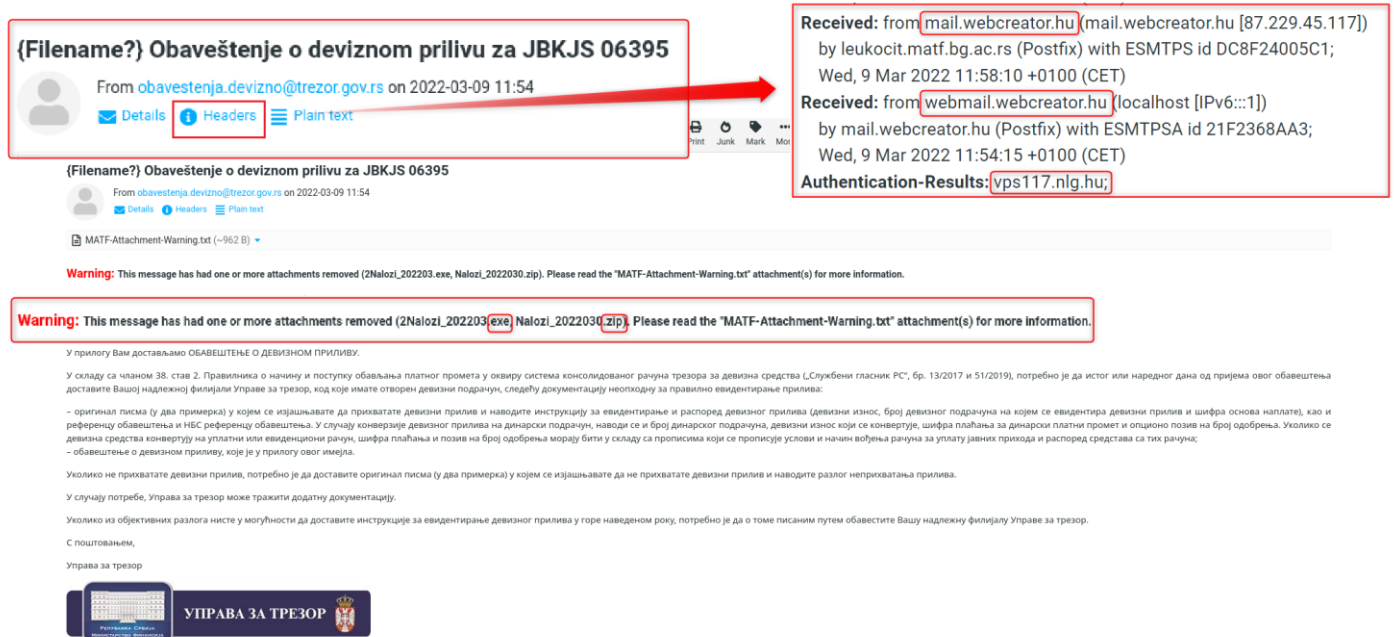
Приказано е-писмо има све до сада поменуте карактеристике кривотворене поште. Пошиљалац је из сектора државне управе (адреса @trezor.gov.rs), ћирилични садржај који нас обавештава о девизном приливу, грб Управе за трезор, и лажни прилог који је део преваре: прилог 2Nalozi_202203 је .exe типа - извршиви фајл, а исти прилог је послат и као .zip фајл.

4. Читајте “Headers” (заглавље) е-писма

Када примите е-писмо које Вам из неког разлога делује сумњиво, али и даље нисте сасвим сигурни - у помоћ Вам може притећи заглавље поруке коју сте примили.

Кликом на “Headers” отвориће се разна текстуална поља у којима се јасно види ко је заправо послао мејл без обзира шта пише у малом заглављу.

На илустративним примерима који следе, уоквирена су поља која су од посебне важности при оцењивању да ли је е-писмо ваљано.



{Filename?} Obaveštenje o deviznom prilivu za JBKJS 06395

From obavestjenja.devizno@trezor.gov.rs on 2022-03-09 11:54

Details Headers Plain text

Received: from mail.webcreator.hu (mail.webcreator.hu [87.229.45.117])
by leukocit.matf.bg.ac.rs (Postfix) with ESMTPS id DC8F24005C1;
Wed, 9 Mar 2022 11:58:10 +0100 (CET)

Received: from webmail.webcreator.hu (localhost [IPv6:::1])
by mail.webcreator.hu (Postfix) with ESMTPS id 21F2368AA3;
Wed, 9 Mar 2022 11:54:15 +0100 (CET)

Authentication-Results: vps117.nlg.hu;

Warning: This message has had one or more attachments removed (2Nalozi_202203.exe, Nalozi_2022030.zip). Please read the "MATF-Attachment-Warning.txt" attachment(s) for more information.

У прилогу Вам достављамо ОБАВЕШТЕЊЕ О ДЕВИЗНОМ ПРИЛИВУ.

У складу са чланом 38. став 2. Правилника о начину и поступку обављања платног промета у оквиру система консолидованог рачуна трезора за девизна средства („Службени гласник РС”, бр. 13/2017 и 51/2019), потребно је да истог или наредног дана од пријема овог обавештења доставите Вашој надлежној филијали Управе за трезор, код које имате отворен девизни подрачун, следећу документацију неопходну за правилно евидентирање прилива:

- оригинал писма (у два примерка) у којем се изјашњава да прихватате девизни прилив и наводите инструкцију за евидентирање и распоред девизног прилива (девизни износ, број девизног подрачуна на којем се евидентира девизни прилив и шифра основа наплате), као и референцу обавештења и НБС референцу обавештења. У случају конверзије девизног прилива на динарски подрачун, наводи се и број динарског подрачуна, девизни износ који се конвертује, шифра плаћања за динарски платни промет и опционо позив на број одобрења. Уколико се девизна средства конвертују на уплатни или евиденциони рачун, шифра плаћања и позив на број одобрења морају бити у складу са прописима који се прописује услови и начин вођења рачуна за уплату јавних прихода и распоред средстава са тих рачуна;
- обавештење о девизном приливу, које је у прилогу овог мејла.


Уколико не прихватате девизни прилив, потребно је да доставите оригинал писма (у два примерка) у којем се изјашњава да не прихватате девизни прилив и наводите разлог неприхватања прилива.

У случају потребе, Управа за трезор може тражити додатну документацију.

Уколико из објективних разлога нисте у могућности да доставите инструкције за евидентирање девизног прилива у горе наведеном року, потребно је да о томе писаним путем обавестите Вашу надлежну филијалу Управе за трезор.

С поштовањем,

Управа за трезор

 **УПРАВА ЗА ТРЕЗОР**

Приказани пример на слици изнад је управо последњи наведен у прошлом одељку, док је на слици ниже отворено пуно заглавље где је у пољима “Received” приказано да е-писма не потичу са сервера Управе за трезор нити са неког другог сервера из наше земље.

Следи слика пуног заглавља са уоквиреним и увећаним најважнијим пољима.

Message headers

Return-Path: <srs0=18vu=6d=rect.bg.ac.rs=office@interlan.ro>

Delivered-To: matf@matf.bg.ac.rs

Received: from poincare.matf.bg.ac.rs
by poincare.matf.bg.ac.rs with LMTP
id e0d1KKxJ4m07OCMARjmPpg
(envelope-from <srs0=18vu=6d=rect.bg.ac.rs=office@interlan.ro>
for <matf@matf.bg.ac.rs>; Tue, 07 Feb 2023 13:53:00 +0100 (CET))

Received: by poincare.matf.bg.ac.rs (Postfix, from userid 1000)
id 95DFFA00811; Tue, 7 Feb 2023 13:53:00 +0100 (CET)

Received: from leukocit.matf.bg.ac.rs (leukocit.matf.bg.ac.rs)
by poincare.matf.bg.ac.rs (Postfix) with ESMTTP id 7AFFE
Tue, 7 Feb 2023 13:53:00 +0100 (CET)

Received: from mail.interlan.ro (unknown [195.95.178.25])
by leukocit.matf.bg.ac.rs (Postfix) with ESMTTP id 50E897722CE
Tue, 7 Feb 2023 13:57:42 +0100 (CET)

Received: from mail.interlan.ro (localhost [127.0.0.1])
by mail.interlan.ro (Postfix) with ESMTTP id 50E897722CE
Tue, 7 Feb 2023 14:41:40 +0200 (EET)

MIME-Version: 1.0

Content-Type: multipart/mixed;
boundary="=_e7df61b45565a20bed667e8bb9ea009"

Date: Tue, 07 Feb 2023 13:41:40 +0100

From: =?UTF-8?Q?=D0=A3=D0=B0=D0=B8=D0=B2=D0=B5=D1=80=D0=B7=D0=B8=D1=82?=
=?UTF-8?Q?=D0=B5=D1=82_=D1=83_=D0=91=D0=B5=D0=BE=D0=B3=D1=80=D0=B0=D0=B4?=
=?UTF-8?Q?=D1=83?= <office@rect.bg.ac.rs>

To: undisclosed-recipients;

Subject: =?UTF-8?Q?=D0=97=D0=90=D0=A5=D0=A2=D0=95=D0=92_=D0=97=D0=90_?=
=?UTF-8?Q?=D0=9F=D0=9E=D0=9D=D0=A3=D0=94=D0=90=5FPO=2E30525-7=2E2=2E2023_?=
=?UTF-8?Q?=28=D0=A3=D0=BD=D0=B8=D0=B2=D0=B5=D1=80=D0=B7=D0=B8=D1=82=D0=B5?=
=?UTF-8?Q?=D1=82_=D1=83_=D0=91=D0=B5=D0=BE=D0=B3=D1=80=D0=B0=D0=B4=D1=83?=
=?UTF-8?Q?=29?=

In-Reply-To: <9f7374f3229d80949b4fc925d10e6d1e@batono.ge>

References: <231c7d7ce2e9ce2a17e839f502b77586@moderne1.ml>
<9f7374f3229d80949b4fc925d10e6d1e@batono.ge>

Message-ID: <8732c0ac6b72445fac56d80c5a6fcae1@rect.bg.ac.rs>

X-Sender: office@rect.bg.ac.rs

User-Agent: Roundcube Webmail/1.3.6

X-MATF-MailScanner-Information: Please contact the

X-MATF-MailScanner-ID: C65CF40023B.A191E

X-MATF-MailScanner: Found to be clean

X-MATF-MailScanner-SpamCheck: not spam (too larg

X-MATF-MailScanner-From: srs0=18vu=6d=rect.bg.ac

X-Spam-Status: No

In-Reply-To: <9f7374f3229d80949b4fc925d10e6d1e@batono.ge>

References: <231c7d7ce2e9ce2a17e839f502b77586@moderne1.ml>
<9f7374f3229d80949b4fc925d10e6d1e@batono.ge>

Message-ID: <8732c0ac6b72445fac56d80c5a6fcae1@rect.bg.ac.rs>

X-Sender: office@rect.bg.ac.rs

Close

5. Уочите структуру исправног е-писма од администратора веб-сервера

На крају, даћемо још пар савета како да препознате мејл који је послао неко од запослених из Рачунарске лабораторије (са адресе admin@matf.bg.ac.rs пишемо појединачне мејлове запосленима, а са matf@matf.bg.ac.rs свим запосленима/наставницима/пензионерима).

- а) Уводни део е-писма увек садржи “Драге колегинице/колеге”.
- б) Е-писмо нема очигледних граматичких и правописних грешака.
- в) У е-писму Вас не обавештавамо да ће доћи до брисања или суспендовања налога.
- г) Е-писмо никада не садржи линкове или дугмад на коју треба кликнути да би дошло до решавања неког проблема.
- д) Е-писмо никада не захтева било какво уношење података нити друге активности којима би налог остао активан.
- ђ) У потпису је увек пуно име и презиме запосленог из Рачунарске лабораторије који је упутио мејл.

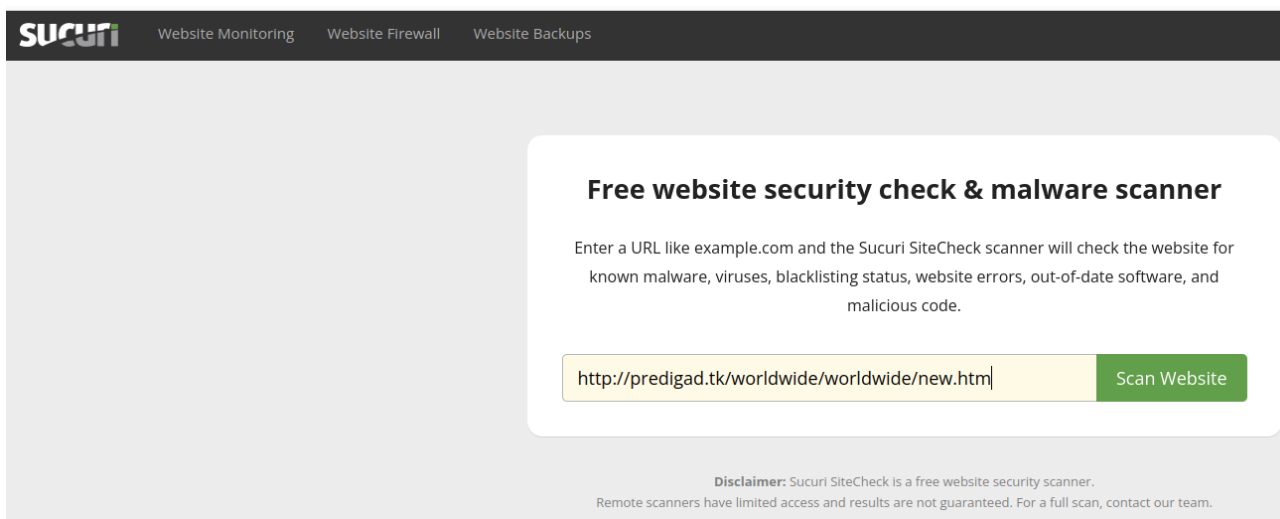
У случају да савети нису довољни да е-писмо класификујете као непожељно или злонамерно, а ипак делује сумњиво - проследите га као и слику целог заглавља на admin@matf.bg.ac.rs.

6. Провера малициозности Веб сајта чија посета Вам је предложена у фишинг е-поруци

Пецање се често изводи путем е-поште која садржи хипервезу ка вешто креираној страници која је толико уверљива да недовољно опрезан посетилац не може да разликује лажан и малициозни сајт од правог сајта.

Провера малициозност неког сајта се може поверити бесплатним алатима:

1. <https://sitecheck.sucuri.net/>



Резултат скенирања Веб сајта

Website Blacklist Status

⚠ Domain blacklisted by Google Safe Browsing:
<http://predigad.tk/worldwide/worldwide/new.htm>

⚠ Domain blacklisted by McAfee:
<http://predigad.tk/worldwide/worldwide/new.htm>

Проверите статус сајта

<http://predigad.tk/worldwide/worldwide/new.htm>



Актуелни статус

Овај сајт није безбедан

Сајт <http://predigad.tk/worldwide/worldwide/new.htm> садржи штетан садржај, укључујући странице које:

- Покушавају да преваре посетиоце да деле личне податке или преузму софтвер

Шта треба да урадите

• Не паничите.

Chrome и други Google производи имају уграђене безбедносне функције које вас штите током прегледања. [Сазнајте више.](#)

• Заштитите се.

Информације о томе како да се заштитите од штетних сајтова потражите у [Google центру за безбедност](#).

• Потражите помоћ

У чланцима [помоћи за власнике веб-сајтова у вези са Безбедним прегледањем](#) сазнајте како да очистите сајт и заштитите га од будућих напада.

Информације о сајту

Ове информације су последњи пут ажуриране 11. нов 2022..

Безбедност сајта може временом да се промени. Вратите се да бисте видели да ли постоје ажурирања.

2. <https://transparencyreport.google.com/safe-browsing/search>

3. <https://quttera.com/>



 Scan website for free

<https://predigad.tk/worldwide/worldwide/new.htm>

Enter URL

Scan for Malware >

Now scanning: 10 websites

7. Како да сами препознате малициозни сајт

7.1. Пажљиво погледајте УРЛ

Адресна трака у прегледачу садржи информације о томе где се налазите и колико сте безбедни.

Стратегија аутора фишинг сајтова је да креирају страницу која се готово не разликује од праве, легитимне странице. Сајбер криминалци креирају поддомене који опонашају праве домене, а сервиси за скраћивање УРЛ-а могу да маскирају реалне адресе.

7.2. WHO.IS база података помаже откривање лажних сајтова

Ако желите да знате ко управља сајтом, односно доменом на ком је смештен сајт, можете проверити званичну регистрацију сајта преко WHO.IS регистрација: **<https://who.is/>**.

WHO.IS регистрација вам може рећи ко је власник сајта и да ли је у питању појединац или организација. Уколико је у питању компанија, писаће "Organization" заједно са адресом и бројем телефона. Уколико је у питању појединац, писаће "Name" заједно са адресом.

Уколико на неком сајту пише да је у власништу велике компаније, али је адреса регистрована у другој држави, велика је шанса да сте на лажном сајту.

Хвала на интересовању и жељи да сачувате мејл сервер нашег факултета!