УПУТСТВО ЗА ЗАШТИТУ ОД ЕМАИЛ PHISHING НАПАДА

Емаил phishing напади су облик cyber-напада у којима нападачи користе лажне емаил-ове како би преварили кориснике и навели их да открију своје личне податке, лозинке, или финансијске информације. Да бисте се заштитили од оваквих напада, пратите сљедеће савјете:

1. Препознајте phishing емаил

- **Провјерите адресу пошиљаоца:** Нападачи често користе адресе које личе на легитимне, али су мало измијењене. На пример, уместо example@company.com, могу користити example@compaany.com. Нападачи воле имитирати институције, системе и услуге. Поље пошиљаоца може бити лажирано! И са легитимне адресе може стићи phishing емаил, зато обратите пажњу на садржај емаила.
- **Погледајте садржај емаила:** Будите сумњичави према емаил-овима који захтијевају хитну акцију, пријете посљедицама или нуде невјероватне награде. Не уплаћујте новац ни криптовалуте особама које су те контактирале путем емаил-а. Ако сте у недоумици, директно контактирајте компанију или особу која је наводно послала емаил.
- **Провјерите грешке у граматици и правопису:** Phishing емаил-ови често садрже грешке у граматици и правопису.
- **Провјерите линкове:** Пре него што кликнете на било који линк, пређите мишем преко њега како бисте видјели праву адресу на коју води. Ако адреса изгледа сумњиво, немојте кликнути. Нападач ће те покушати навести на злонамјерну веб страницу на којој ће ти тражити унос личних података (нпр. података банковне картице). Иако страница може изгледати легитимно, она је вјероватно направљена са циљем крађе личних података.
- **Опасност из прилога:** Ако вам је непознат пошиљалац, сумњив садржај емаил-а, и нуди вам и прилог емаил-а велика је вјероватноћа да је у прилогу неки облик вируса.

2. Обезбиједите своје податке

- **Никада не дијелите личне информације преко емаил-а:** Легитимне установе, компаније никада неће тражити ваше лозинке или банковне информације путем емаил-а.

3. Обезбедите свој уређај и мрежу

- **Користите антивирусни програм:** Редовно ажурирајте антивирусни софтвер како бисте заштитили свој уређај од злонамијерног софтвера.
- **Ажурирајте оперативни систем и софтвер:** Редовна ажурирања помажу у затварању сигурносних рупа које нападачи могу искористити.
- **Користите сигурне мреже:** Избегавајте повезивање на непознате или несигурне Wi-Fi мреже, посебно када приступате осјетљивим информацијама.

ПРИМЈЕРИ НАПАДА PHISHING - ПЕЦАЊЕМ

ПРИМЈЕР 1

From: Admin office [mailto:univertet@ues.rs.ba] [1]
Sent: Tuesday, January 14, 2023 2:48 PM
To: Recipients <univertet@ues.rs.ba>
Subject: Rector of the University of East Sarajevo

Poštovani korisniče e-pošte:

Uočili smo da vaša e-pošta nije prošla postupak verifikacije / ažuriranja na kojem trenutno radimo[2].
Trenutno nadograđujemo našu bazu podataka i centar za e-poštu.

Da biste spriječili da se vaš račun zatvori / izbriše i da mu se omogući i najviša internetska sigurnost ikad, morat ćete ga ažurirati tako da ćemo znati da se radi o sadašnjem korištenom računu. Da biste dovršili ponovno potvrđivanje računa, molimo kliknite OVDJE[3]

Hvala ti

Centar za podršku administratora

© 2020 Webmail Administrator. Sva prava zadržana.
Prilog: Placanje.xls, Nalog.pdf, Prijava.docx, Uplata.jpg, Nagrada.rar, Dekan.zip, BankaUplata.pdf [4].

ПРЕГЛЕД НАПАДА ПРИМЈЕР 1

- Непознат емаил. У пристиглом емаил-у видимо непознату емаил адресу у пољу From : [mailto:univertet@ues.rs.ba][1]. Одмах закључујемо да је емаил потенцијална превара. Ако вам изгледа да је емаил регуларан наставите даље са прегледавањем садржаја емаил-а. И са легитимне адресе може стићи phishing линк спам порука и слично, зато обратите пажњу на садржај емаила.
- У овом случају измислили су акцију верификације / ажурирања[2]. Администратори емаил система Универзитета у Источном Сарајеву не шаљу корисницима службеног емаил-а обавјештења да верификују лозинку, налог, упозорење да су им поруке на чекању, недостатак меморије и слично. Када видите да то пише одмах знате да се ради о превари.
- Лажни линк[3]. У емаил-у вас наводе на кликнете phishing линк (лажну страницу - https://xxues-rs-ba-organizacija-rektor-univerziteta.weebly.com/) која садржи поља за унос корисничког имена и лозинке. Ако унесете тражене податеке у форму на понуђеној страници, ви сте тада послали своју лозинку злонамјерним особама, и преварени сте – упецани.
- Прилог [4]. У прилогу емаил-а је заражени фајл. Ако преузмете и отворите фајл он се инсталира у ваш рачунар и онда може да преузме ваше податке, лозинке, закључа вам све фајлове, обрише фајлове у зависности од његових могућности. Ако вам је непознат пошиљалац, сумњив садржај емаил-а, и нуди вам и прилог емаил-а велика је вјероватноћа да је у прилогу неки облик вируса.

Након уоченог лажног - непознатог емаил-а, могли смо одмах закључити да је емаил превара.

Даљим прегледом смо утврдили и измишљену верификацију.

Понудили су и лажни линк у овом случају https://xxues-rs-ba-organizacija-rektor-univerziteta.weebly.com/

Понуђени прилог садржи највјероватније вирусе.

ПРИМЈЕР 2

From: Administrator [mailto:admin@ues.rs.ba]
Sent: Tuesday, January 14, 2023 3:48 PM
To: Recipients <univertet@ues.rs.ba>
Subject: Poruke nisu isporučene[1]

Здраво

имате долазну поруку од кабинет ректора проф. др Милана Кулића љубазно кликните овде да прочитате[2]

Хвала вам.
Админ

кабинета ректор проф. др Милана Кулића

Универзитет у Источном Сарајеву

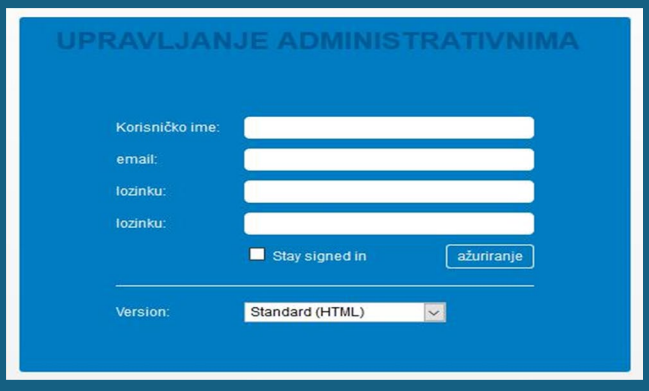
ПРЕГЛЕД НАПАДА ПРИМЈЕР 2

- Изгледа као да је емаил регуларан admin@ues.rs.ba наставите даље са прегледавањем садржаја емаил-а. И са легитимне адресе може стићи phishing линк, спам порука и слично, зато обратите пажњу на садржај емаил-а.
- У овом случају измислили су да поруке нису испоручене[1]. Администратори емаил система Универзитета у Источном Сарајеву не шаљу корисницима службеног емаил-а обавјештења да верификују лозинку, налог, упозорење да су им поруке на чекању и слично. Када видите да то пише одмах знате да је превара.
- Лажни линк[2]. У емаил-у вас наводе на кликнете phishing линк (лажну страницу - https://admin-ba-zimb-up.00x0webhostapp.com/adm/adm/ZimbraWebClientSignIn.html) тј. Веб страницу која садржи поља за унос корисничког имена и лозинке. Ако унесете тражене податеке у форму на понуђеној страници, ви сте тада послали своју лозинку злонамјерним особама, и преварени сте – упецани.

Закључујемо да је превара јер не могу постојати поруке на чекању.

Понудили су лажни линк у овом случају:

https://admin-ba-zimb-up.00x0webhostapp.com/adm/adm/ZimbraWebClientSignIn.html



Subject: Request for Commercial offer - Special Fitting - ADEL/J-80-PI-MRQ-1
عادل- پیشنهاد فنی تقاضای شماره

ПРИМЈЕР 3

Date:01 Jul 2024 10:19:51
From:uis@unssa.rs.ba <uis@unssa.rs.ba>
To:uis@unssa.rs.ba

Blocked incoming messages for urc@unssa.rs.ba

You have 10 pending messages for delivery to your mail box.

Authorize Delivery for pending mails

(c) Poweredby: IT unssa.rs.ba Support.

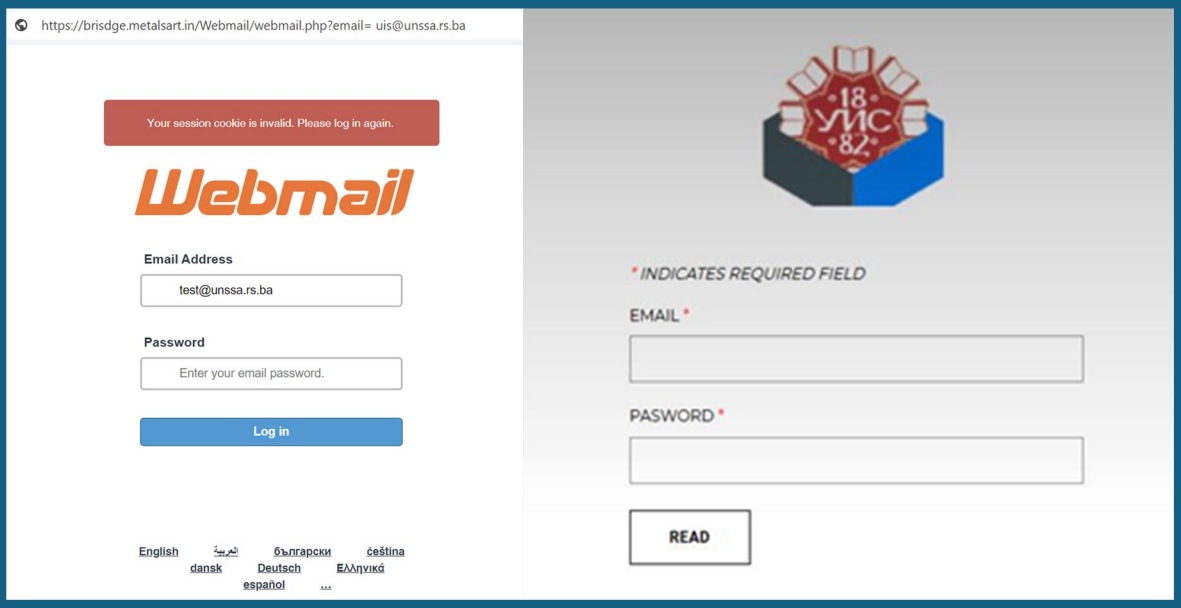
Attachment: Placanje.xls, Document.pdf

ПРЕГЛЕД НАПАДА ПРИМЈЕР 3

- Изгледа као да је емаил регуларан uis@unssa.rs.ba . И са легитимне адресе може стићи phishing линк, спам порука и слично, зато обратите пажњу на садржај емаил-а.
- Превара у виду порука које нису испоручене.
- Лажни линк . Страница која садржи поља за унос корисничког имена и лозинке.
- Прилог. У прилогу емаил-а је заражени фајл.

Закључујемо да је превара јер не могу постојати поруке на чекању.

Понудили су лажни линк у овом случају:
https://brisdge.metalsart.in/Webmail/webmail.php?email=%20uis@unssa.rs.ba



ПРИМЈЕР 4

From: Administrator [mailto: direktor@kasfkasdk.ux.ba]
Sent: Tuesday, January 14, 2024 3:48 PM
To: Recipients <univertet@ues.rs.ba>
Subject: Директор полиције

Здраво

имате долазну поруку од шефа полиције љубазно преузмите документе из прилога, или кликните овдје

Шеф полиције

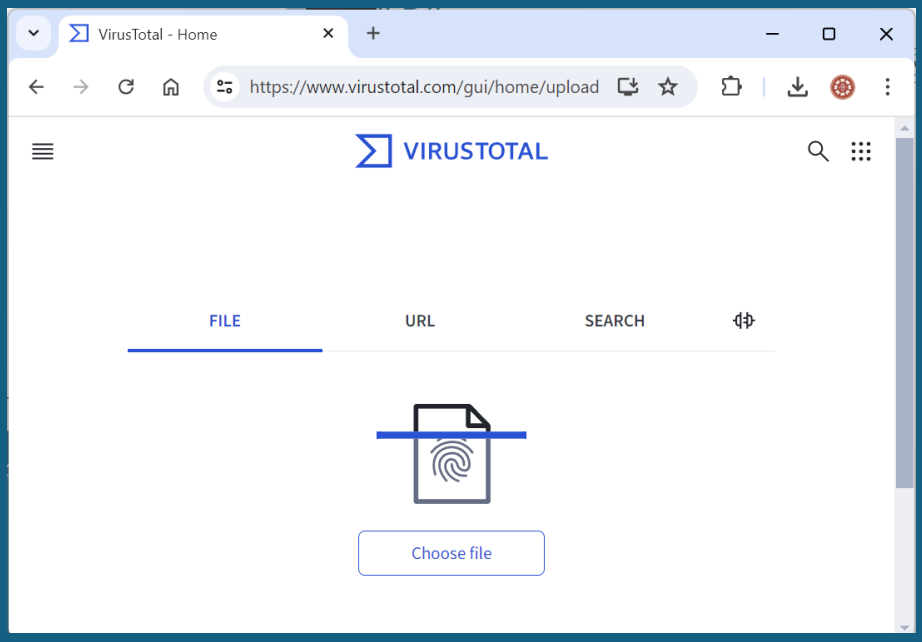
Прилог: Placanje.xls, Nalog.pdf

ПРЕГЛЕД НАПАДА ПРИМЈЕР 4

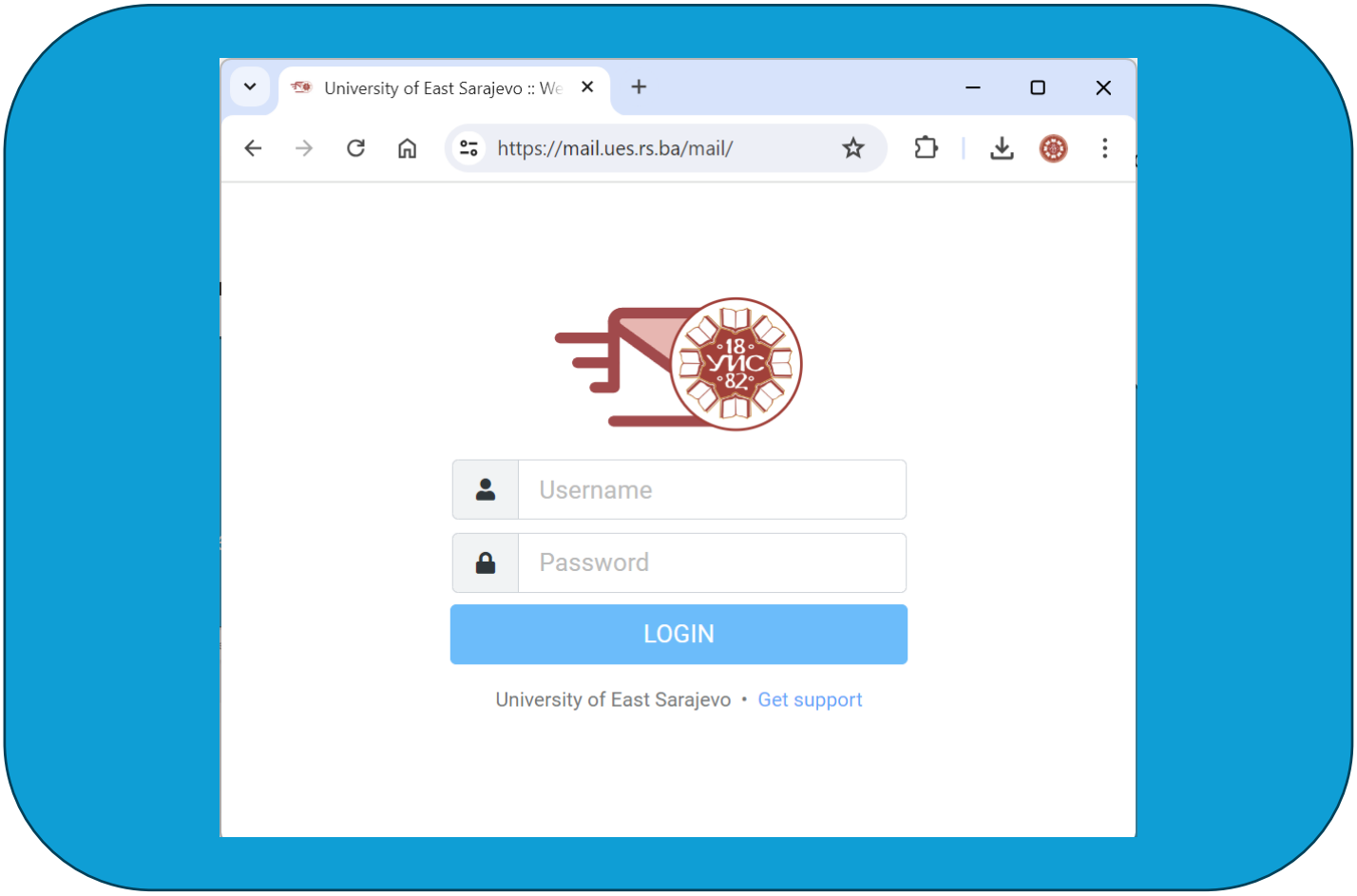
- Непозната емаил адреса: direktor@kasfkasdk.ux.ba .
- Превара у виду поруке од наводног шефа полиције.
- Лажни линк . Отвара се phishing страница која садржи поља за унос корисничког имена и лозинке.
- Прилог. У прилогу емаил-а је заражени фајл.

Закључујемо да је превара јер нисте очекивали поруку од директора полиције. Порука долази са непознате адресе. На линку вам траже да унесете своју лозинку или неке друге личне информације. Пошто нисте очекивали никакву поруку са непознатог емаил-а не отварајте ни прилог јер је велика вјероватноћа да је вирус у прилогу.

Сваки линк или прилог можете тестирати на потенцијално присуство вируса на страници: https://www.virustotal.com



УНИВЕРЗИТЕТСКА СТРАНИЦА ЗА ПРИСТУП ЕМАИЛ-У ИЗГЛЕДА КАО НА НАРЕДНОЈ СЛИЦИ



Поред очигледних разлика у изгледу регуларне и лажних страница, кључна разлика је веб адреса, а легитимне су само:

https://mail.ues.rs.ba/mail

&

https://mail.OJ.ues.rs.ba/mail

OJ префикс који користи Организациона јединица (НПР.: **mail.pof.ues.rs.ba**, **mail.pfb.ues.rs.ba** и сл.)

Препознајте phishing емаил

- **Провјерите адресу пошиљаоца**
- **Пажљиво прегледајте садржај емаил-а**
- **Грешке у граматици и правопису указују на могућност преваре и лажног представљања**
- **Провјерите линкове**
- **Прилог може да садржи опасне вирусе**