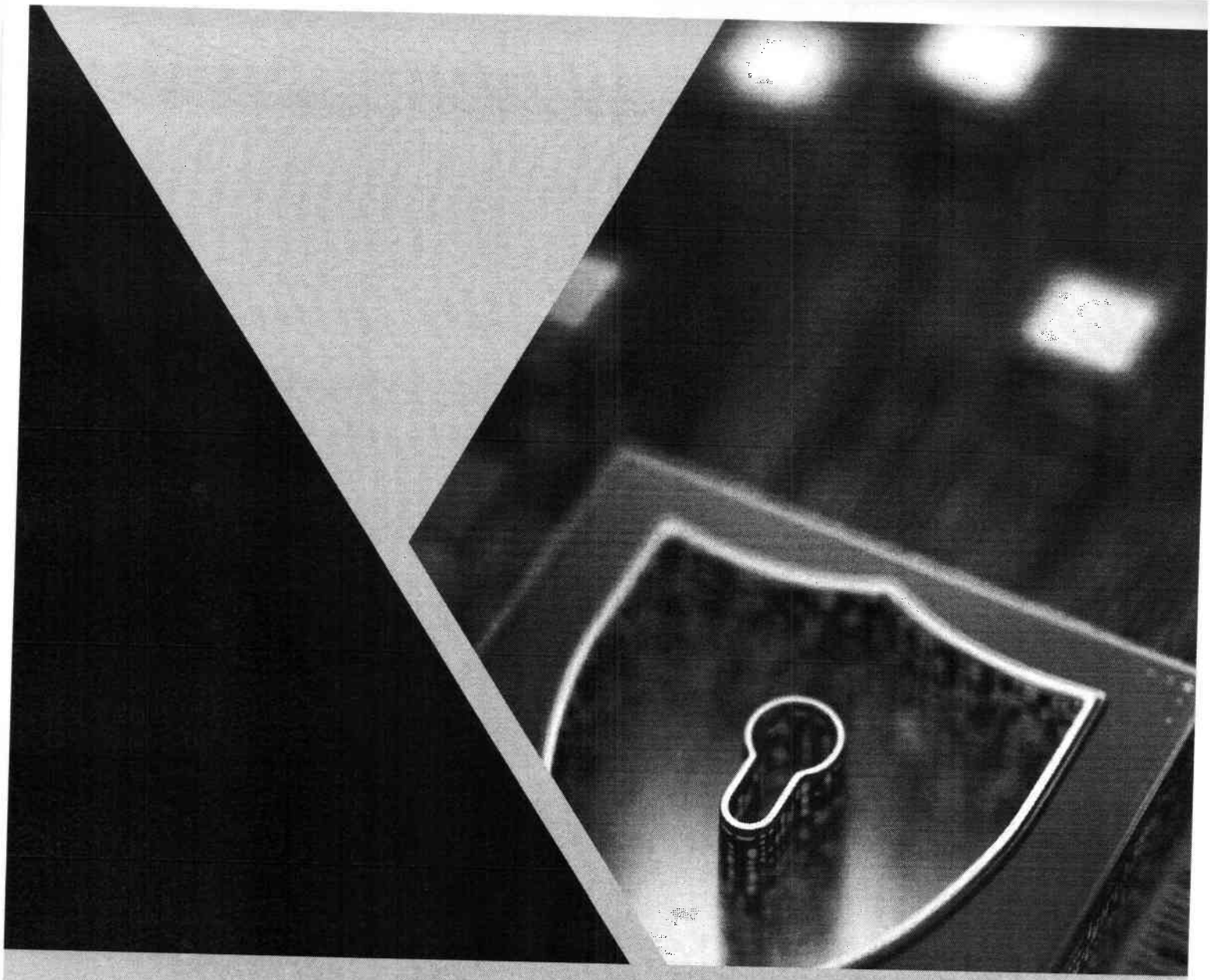
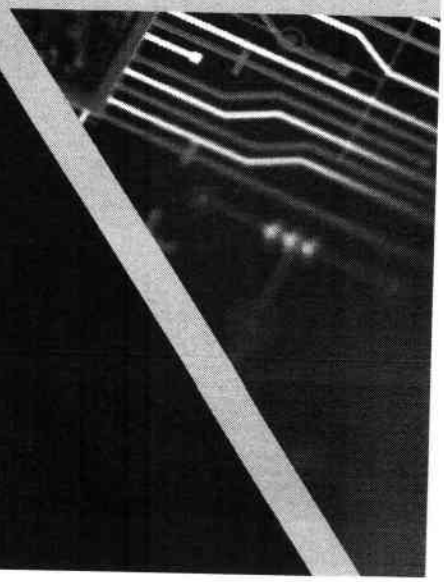
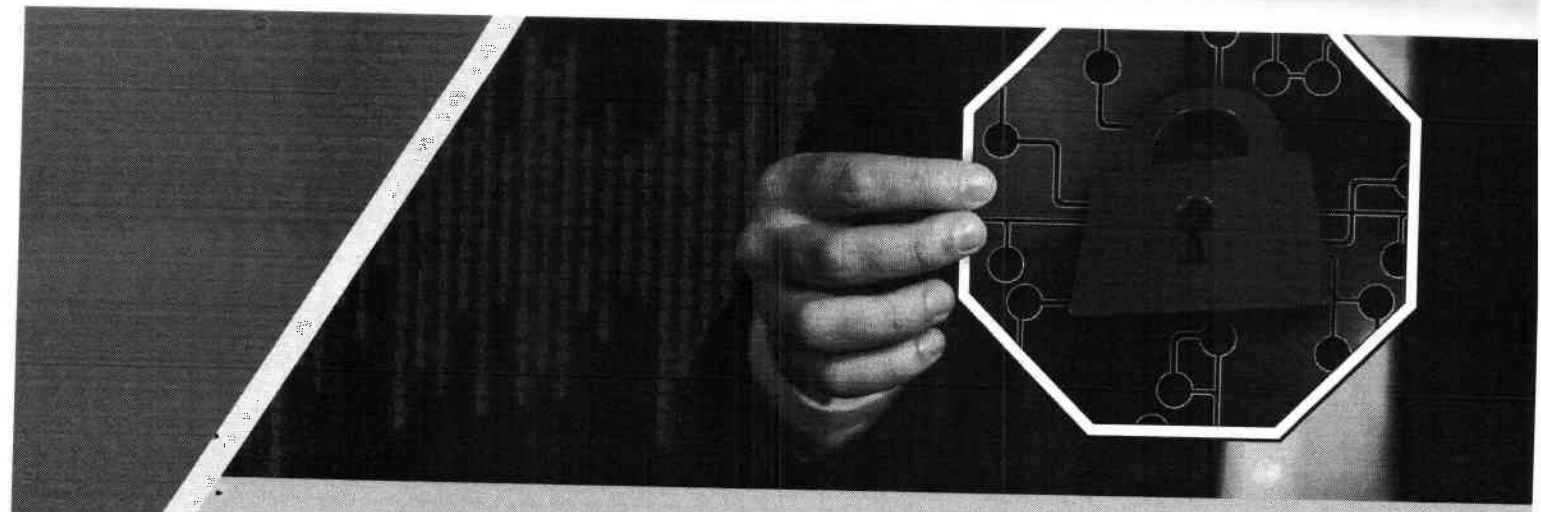


# БЕЗБЕДНОСТ НА **ИНТЕРНЕТУ**

*Основе коришћења интернета*



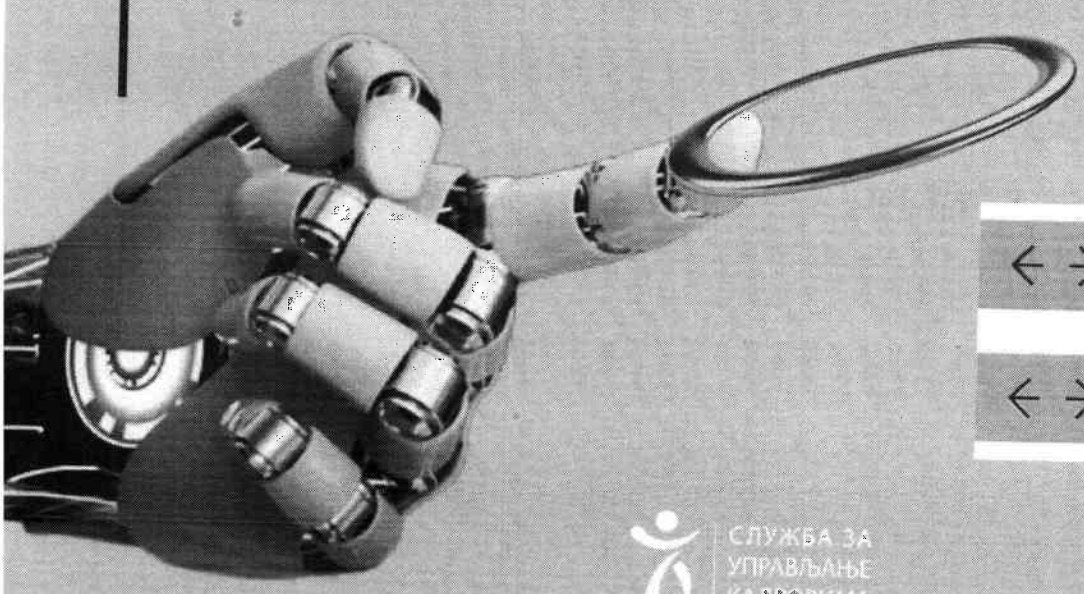
СЛУЖБА ЗА
УПРАВЉАЊЕ
КАДРОВИМА

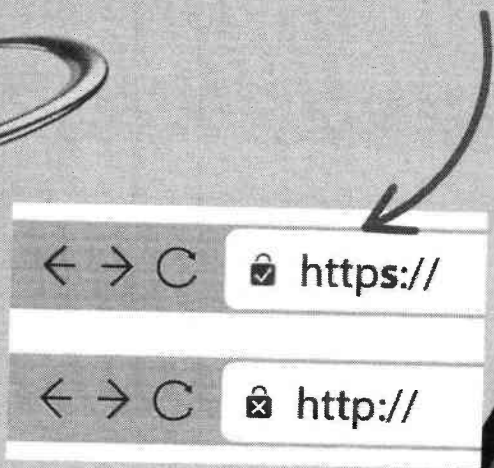


# *HTTPS vs. HTTP – Зашто је битно?*

Замислите да се пријављујете на своју банку путем интернетског претраживача. Ако видите да URL почиње са **http://** уместо https://, то значи да је сајт **незаштићен.** Нападачи могу пресрести ваше податке и украсти вашу лозинку.

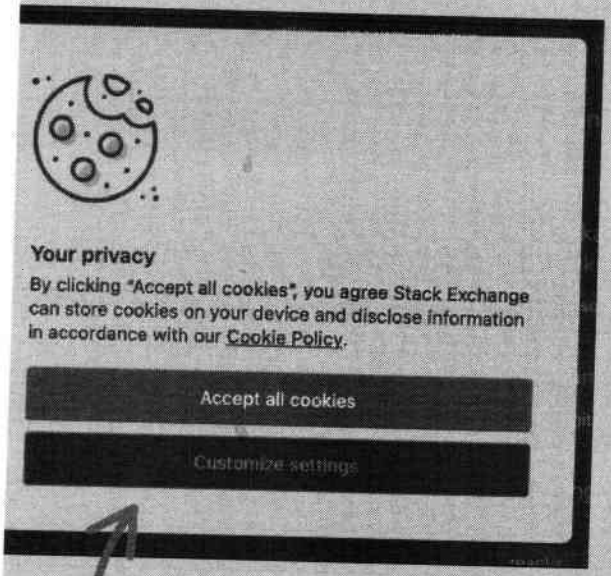
Увек проверите URL сајта – ако видите https:// на почетку, сајт користи енкрипцију и безбедан је за унос личних података. Ако је http://, сајт није заштићен и препоручујемо да **не уносите** осетљиве податке.





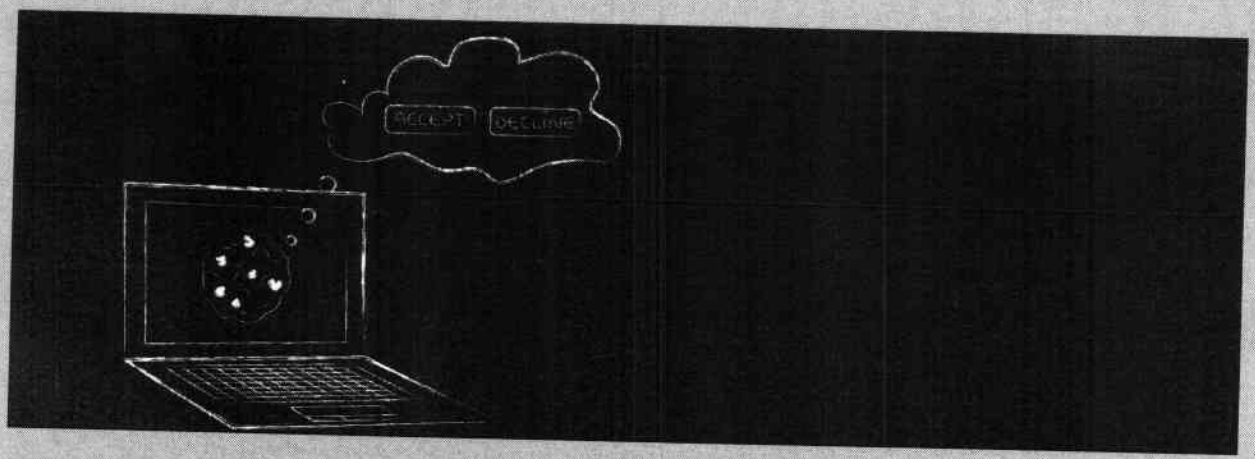

СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА

# *Шта су колачићи (cookies) и како раде?*

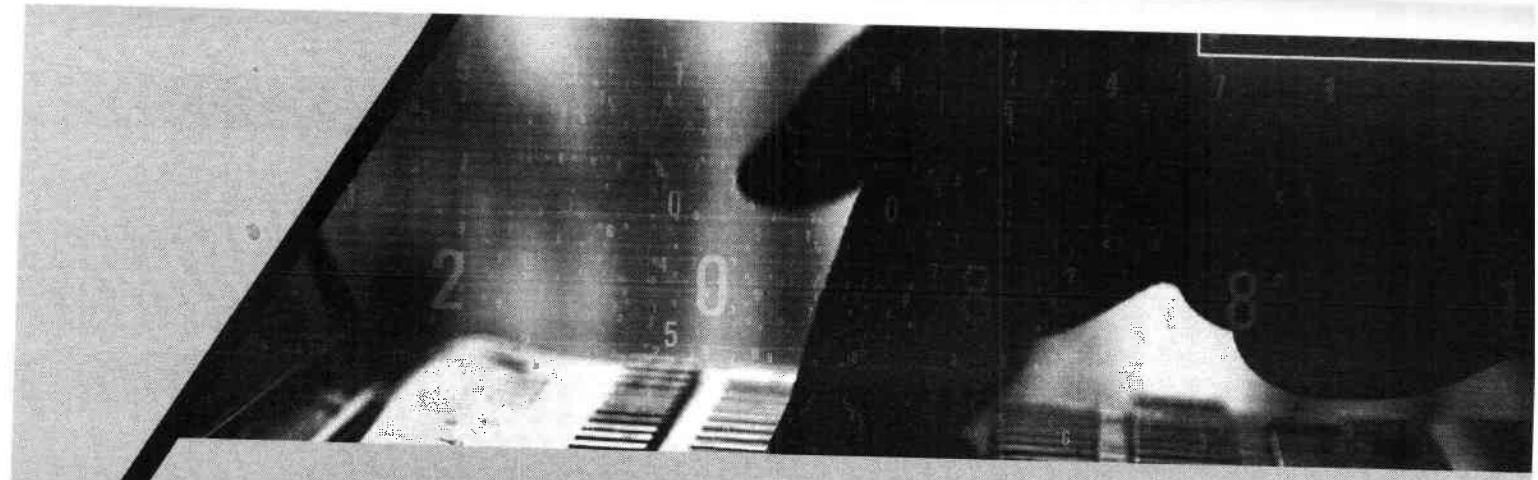



Када посетите сајт за онлајн куповину, може вам бити понуђено да прихватите колачиће како бисте „паметно" бирали производе на основу претходних посета. Док је ово корисно, колачићи могу пратити ваше понашање на интернету. Ако сте **забринути** због приватности, можете искључити колачиће у поставкама претраживача.

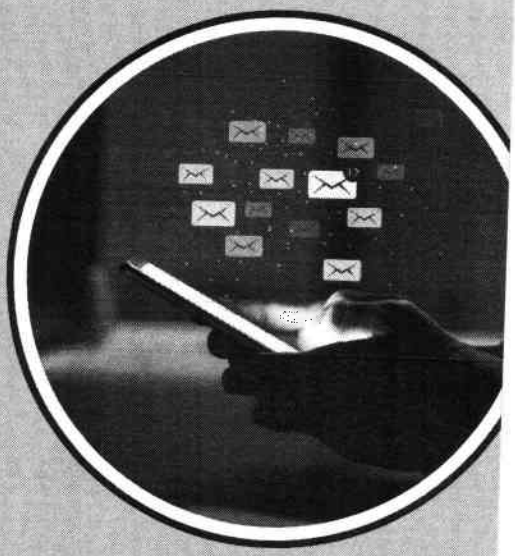
Колачићи помажу сајтовима да **запамте** ваше преференције и понашање, али могу бити коришћени и за праћење ваших активности. Редовно бришите колачиће са свог уређаја и **пазите** на сајтове који захтевају приступ свим колачићима. Ако желите **већу контролу** над приватношћу, поставите свој претраживач да аутоматски блокира колачиће трећих страна.



СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА

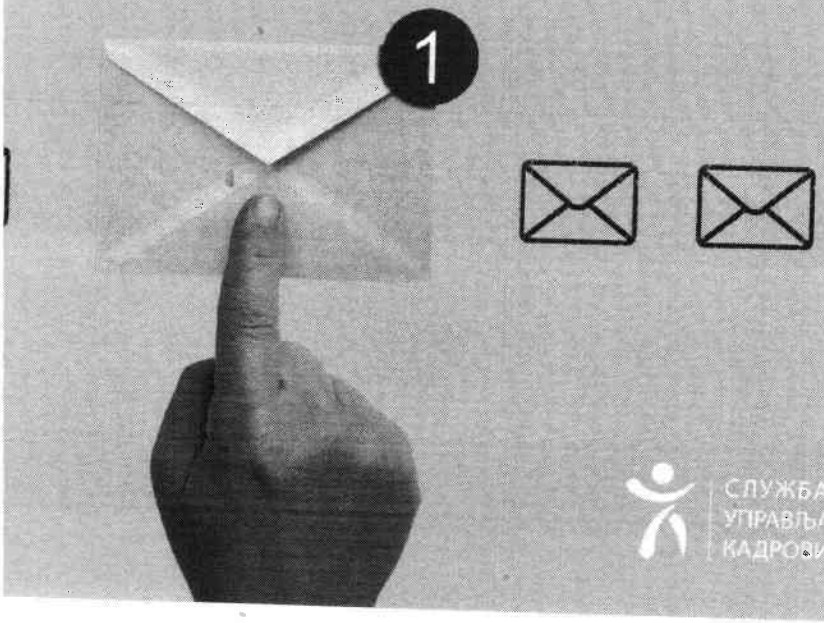


# Малициозни мејлови (phishing) – Како их препознати?



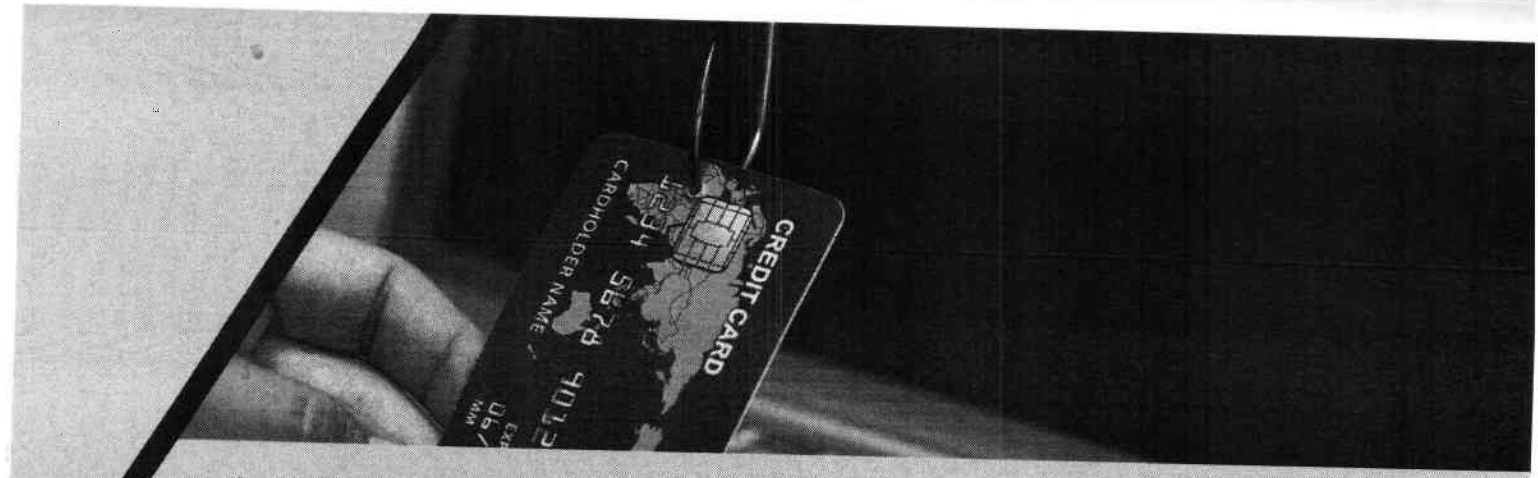
**❗ *Превара која изгледа као званични захтев за промену података***

„Поштовани господине/госпођо,
Обавештавамо Вас да је ваш налог на корпоративном порталу привремено блокиран због безбедносних разлога. Да бисте поново добили приступ, молимо вас да унесете своје нове пријавне податке у следећем формулару: [сумњиви линк].
Хвала вам што брзо решавате ову ситуацију.
С поштовањем,
Тим за подршку"




***Никада не улазите на линкове из непознатих или сумњивих мејлова. Пре него што унесете било какве податке, увек се уверите да сте добили мејл са званичне адресе компаније. Ако имате било каквих сумњи, контактирајте ИТ или безбедносни тим компаније директно.***

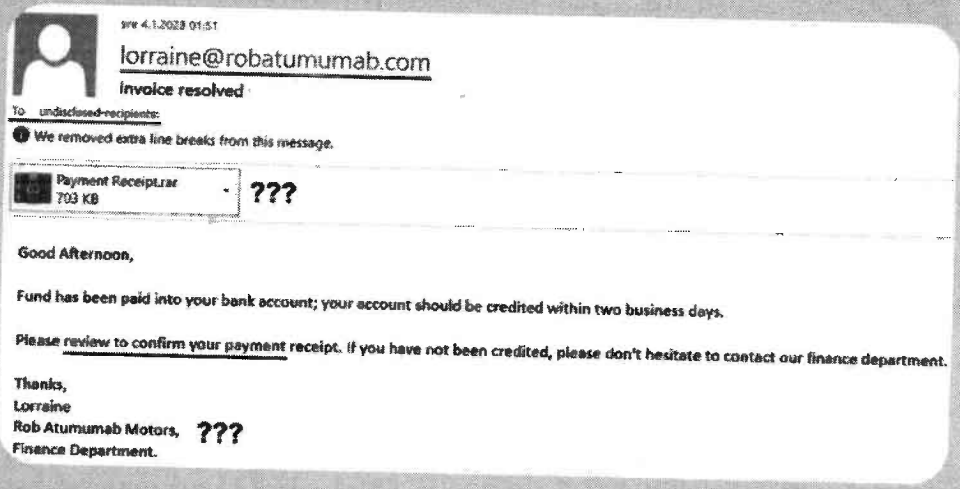
СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА




# Малициозни мејлови (phishing) – Како их препознати?

### ❗ *Лажни захтев за пренос новца*

„Поштовани,
Молимо вас да одмах извршите трансфер од 10.000 РСД на рачун нашег добављача како бисмо избегли застоје у испоруци. Трансфер мора бити обављен данас, иначе ће бити касно за овогодишње наруџбине.
Детаљи трансфера:
Рачун: [сумњиви подаци]
Хвала на брзом одговору.
С поштовањем,
Финансијски тим"


sre 4.1.2023 01:51

lorraine@robatumumab.com

**Invoice resolved**

To undisclosed-recipients:

We removed extra line breaks from this message.

Payment Receipt.rar
703 KB

???

**Good Afternoon,**

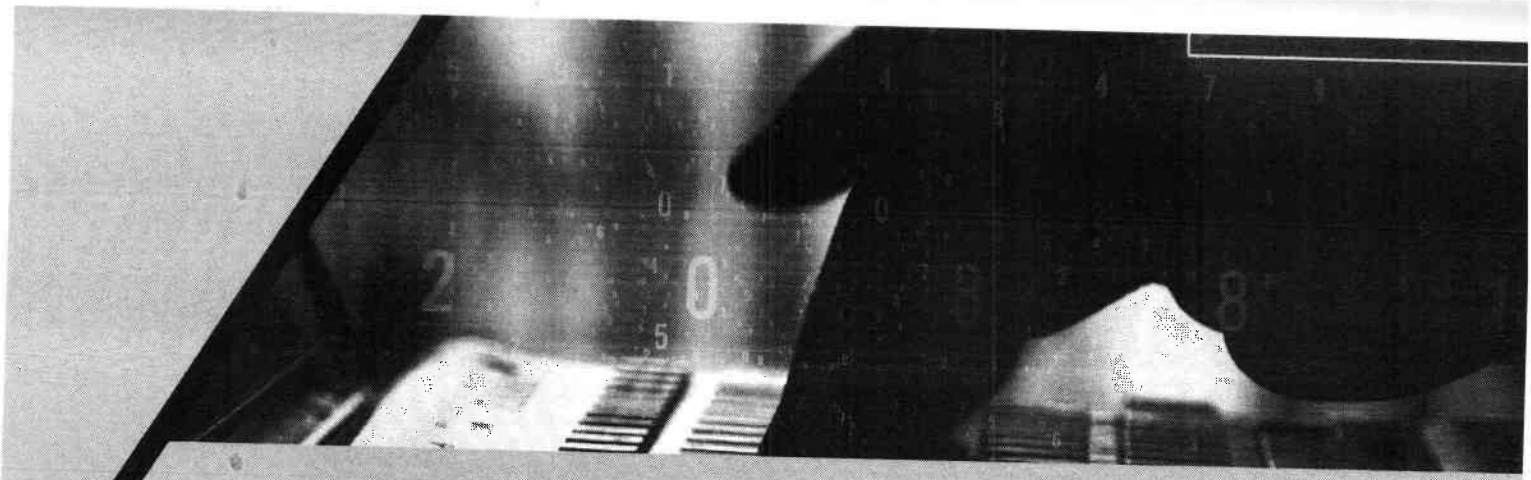
**Fund has been paid into your bank account; your account should be credited within two business days.**

**Please review to confirm your payment receipt. If you have not been credited, please don't hesitate to contact our finance department.**

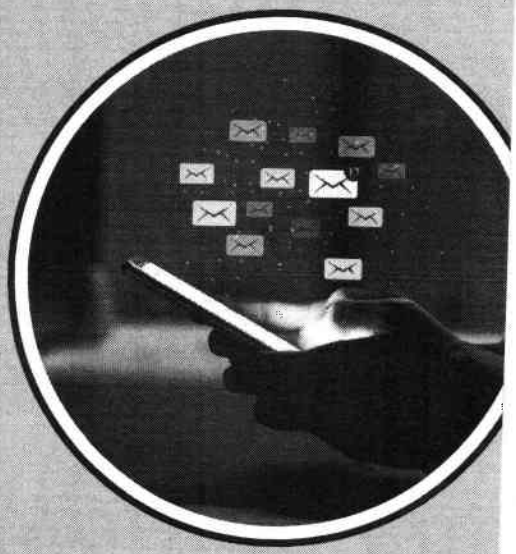
**Thanks,**
**Lorraine**
**Rob Atumumab Motors,** ???
**Finance Department.**

***Ако добијете овако хитне захтеве, увек се уверите да сте добили ову инструкцију од стварне особе у компанији, путем других канала комуникације. Проверите адресе са којих добијате мејлове и не кликајте на линкове који изгледају сумњиво. Увек се консултујте са својим финансијским или рачуноводственим тимом пре него што обавите било какве трансакције.***

СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА



# *Малициозни мејлови (phishing) – Како их препознати?*



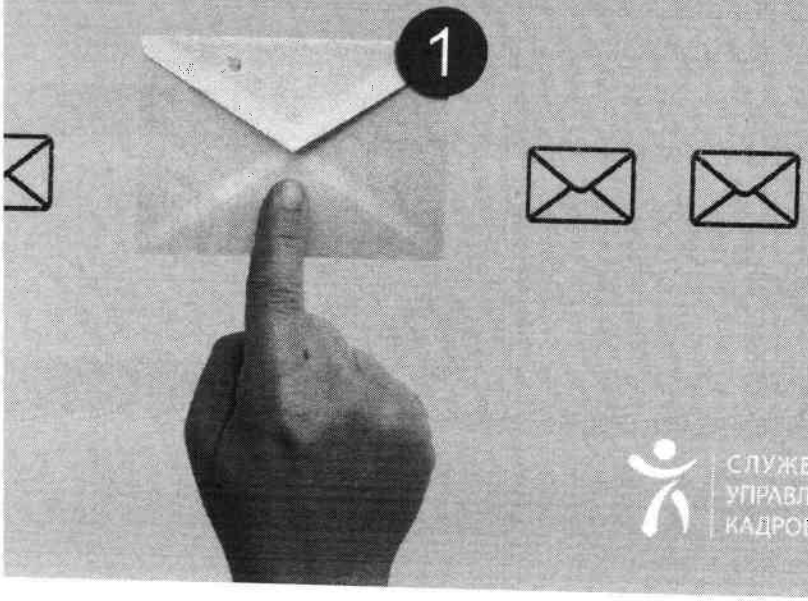
**Мејл банке**

Сви смо бар једном добили мејл који изгледа као да долази од наше банке, иако у ствари није.

„Поштовани,

Ваш банковни рачун је компромитован. Кликните на следећи линк и унесите податке како бисте га заштитили: [сумњиви линк].

Иако изгледа као званичан мејл, овакви мејлови су често превара која покушава да украде ваше податке."




***Малициозни мејлови обично долазе од извора који изгледају познато, али захтевају од вас да предузмете хитну акцију. Проверите да ли је име пошиљаоца тачно, обратите пажњу на граматичке грешке, и немојте кликати на линкове који вам изгледају сумњиво. Ако нисте сигурни, увек проверите са стварним извором (нпр. позовите банку).***

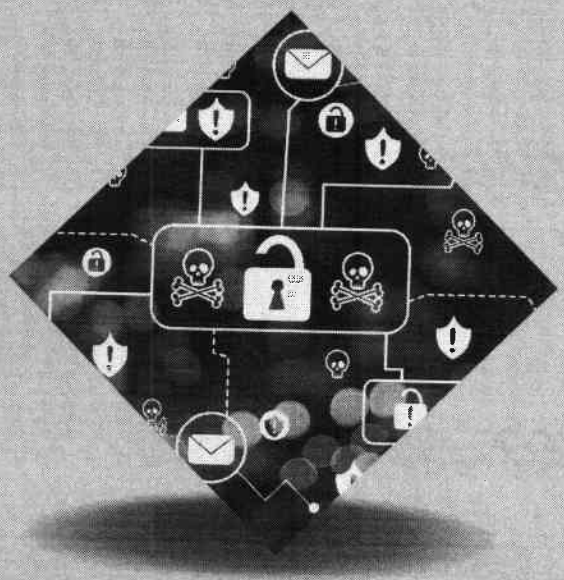
СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА

# *Лажне веб-странице и крађа података*

Приликом куповине на интернету, можда наиђете на сајт који изгледа као званични Amazon или eBay, али **URL** је **сумњив**:

URL: www.amason.com (погрешно написано) уместо www.amazon.com. То је типичан пример лажног сајта који покушава да вас превари.

Лажне веб странице могу изгледати идентично правим, али URL је често суптилно промењен. Увек проверите да ли је URL тачан и да ли је сајт сигуран (HTTPS). Ако нешто изгледа предобро да би било истинито, вероватно није.



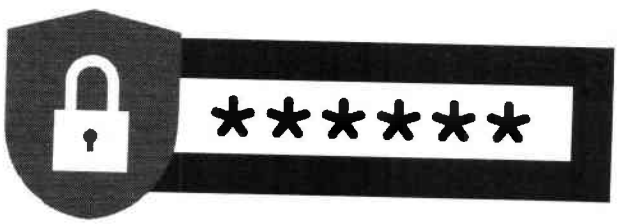
# *Malware и вируси – Како се шире и како их избегавати?*

Можете добити мејл са привитком који се претвара да је PDF документ, али заправо је **malware**. Када отворите фајл, он може заразити ваш рачунар.
**Не отварајте** сумњиве фајлове, поготово ако не очекујете документ од пошиљаоца. Malware се често шири путем привитака у мејловима, а такође може бити присутан у пиратским верзијама софтверских апликација или несигурним преузимањима. Увек користите антивирусни софтвер и преузимајте софтвер само са званичних извора.

## *Користите јаке лозинке и двофакторску аутентификацију*

Замислите да имате лозинку попут „123456" или „password". То су лозинке које су лако погодити и представљају велику сигурносну претњу. Уместо тога, користите сложене лозинке, као што је:
Пример лозинке: „5T!m#2@E7p9" (комбинација великих и малих слова, бројева и специјалних карактера).

Користите **јединствене** и **сложене лозинке** које комбинују велика и мала слова, бројеве и специјалне карактере. Такође, обавезно активирајте двофакторску аутентификацију (2FA) на свим важним налозима (банке, друштвене мреже), како би ваши подаци били додатно заштићени.



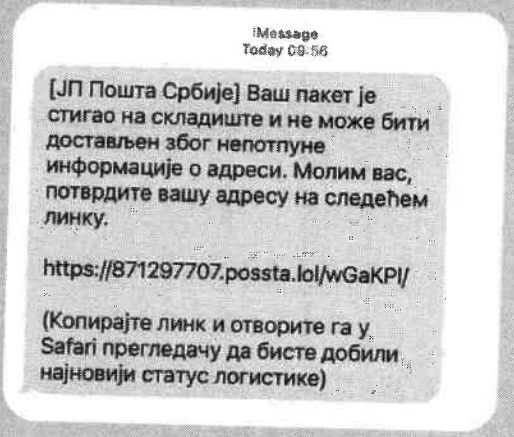

СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА

# БЕЗБЕДНОСТ **ЛИНКА**

Добијате мејл или поруку, који садржи линк:

www.socialnetwork.com/verifyaccount/importantupdate

Пре него што кликнете, проверите да ли је URL заиста **званичан** и да ли садржи исправне информације о друштвеној мрежи.




Никада **не улазите** на линкове из **непознатих** мејлова. Ако желите да проверите линк, пређите мишем преко њега да бисте видели тачан URL. Ако линк изгледа сумњиво, користите алате као што су VirusTotal да бисте проверили безбедност сајта пре него што га отворите.

СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА

# *БЕЗБЕДНОСТ НА* ***ДРУШТВЕНИМ МРЕЖАМА***

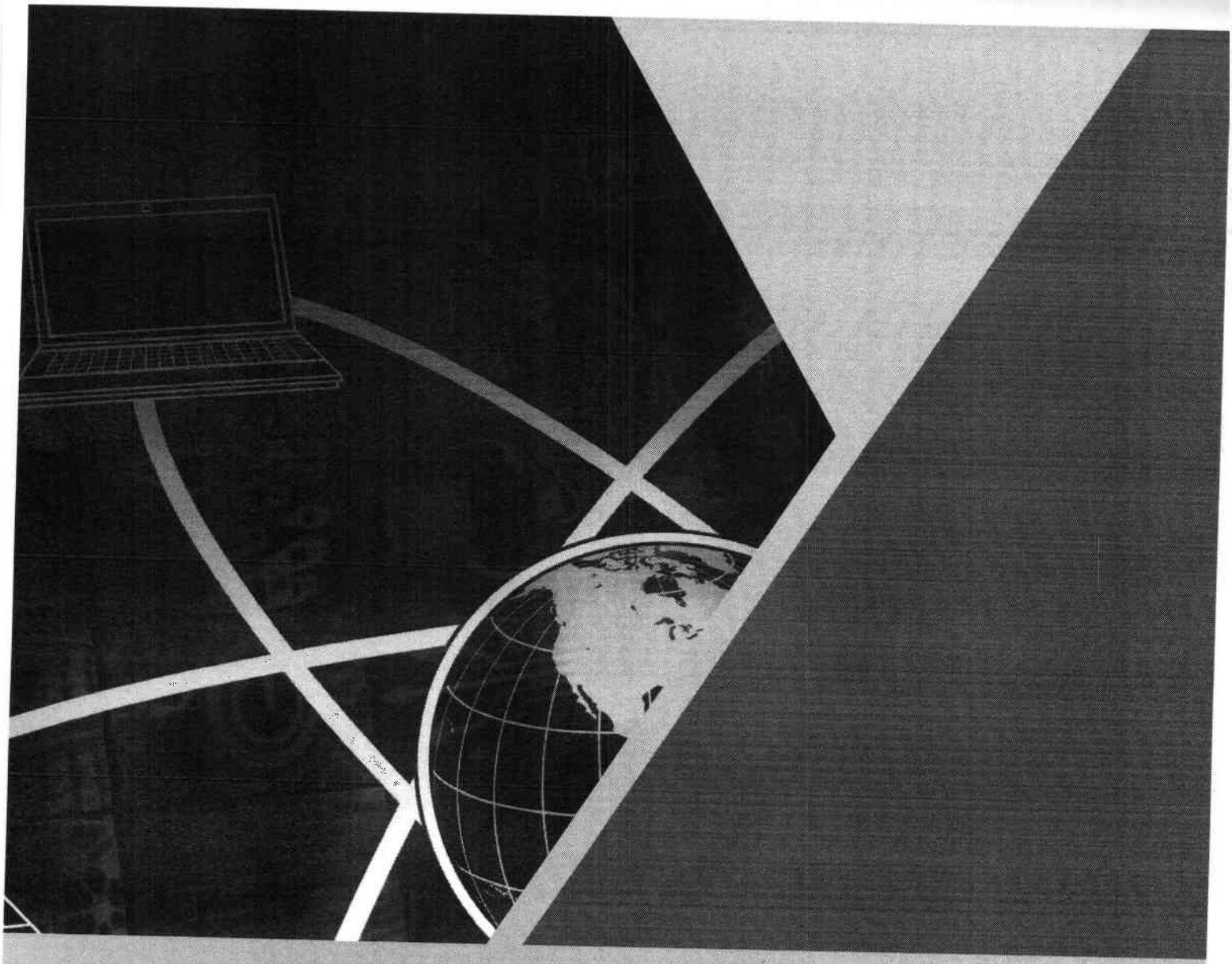
Претпоставимо да неко на друштвеним мрежама шаље захтев за пријатељство и у поруци пише:

„Хеј, погледај ово – ово је баш забавно! [линк]"

Вероватно је ово покушај да вас превари и да вас натера да кликнете на небезбедан линк.


**Будите опрезни са пријатељским захтевима и порукама на друштвеним мрежама. Ако не познајете особу, проверите њен профил и немојте делити личне податке. Такође, поставите високе поставке приватности на својим друштвеним мрежама како бисте контролисали ко може видети ваше објаве.**

СЛУЖБА ЗА УПРАВЉАЊЕ КАДРОВИМА



# БУДИМО **ОПРЕЗНИ!**

СЛУЖБА ЗА
УПРАВЉАЊЕ
КАДРОВИМА