Phishingové emaily
rozpoznanie a obrana

ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Jedným z najefektívnejších nástrojov pre získavanie citlivých informácií zo zabezpečených systémov je sociálne inžinierstvo. Nevyžaduje takmer žiadne technické schopnosti a napriek tomu je s jeho využitím možné exfiltrovať informácie aj z technicky dobre zabezpečených informačných systémov. Je to možné vďaka tomu, že sa tento typ útoku zameriava na jednu z najzávažnejších a najrozšírenejších zraniteľností – na človeka. Jedným z najčastejších spôsobov sociálneho inžinierstva je **phishing**.

Je to typ útoku, pri ktorom sa útočník pokúša získať citlivé informácie prostredníctvom elektronických komunikácií vydávaním sa za dôveryhodnú entitu. Využíva manipuláciu a klamstvo na to, aby od používateľa vylákal prihlasovacie údaje, údaje o kreditných kartách alebo infikoval jeho počítač škodlivým kódom. Phishingové emaily sú koncipované tak, aby pôsobili dôveryhodne a môžu predstierať, že ich odosielateľom sú inštitúcie ako banky, prepravné spoločnosti a iné organizácie, pri ktorých je predpoklad, že s nimi bude mať obeť nejaký vzťah.

Úspešnosť phishingu závisí predovšetkým od dôverčivosti a bezpečnostného povedomia obete, ale aj od bezpečnostných elementov organizácie. Phishing je ale v súčasnosti úspešný predovšetkým kvôli tomu, že kybernetickí kriminálnici sa neustále zlepšujú. Vo phishingových emailoch používajú logá a typografiu organizácie ktorej totožnosť imitujú. Textácia emailov je profesionálna a personalizovaná, a tým aj viac uveriteľná. Používateľa navádza na to, aby otvoril prílohu alebo klikol na odkaz v takomto emaili. Preto je veľmi dôležité všímať si určité znaky na rozoznanie legitímneho emailu od phishingového.

Existuje niekoľko vecí, ktoré by ste si mali všímať na každom emaili, ktorý dostanete:

1. Emailová adresa odosielateľa - či je email odoslaný z neznámej, pochybnej adresy, poprípade skontrolovať adresu, ktorá sa vám zdá známa, ale môže v nej byť nejaký znak pozmenený alebo pridaný.
2. Zvláštna formulácia a zlá gramatika - formulácia viet a pravopisné chyby naznačujúce, že email je prekladaný z cudzieho jazyka automatizovaným nástrojom (google translator a podobne) je jednou zo známok falošnosti emailu.
3. Naliehavosť - výskyt veľkého počtu výkričníkov, časový nátlak na určitú aktivitu (rýchlo zadať údaje, stiahnuť súbor, sankcia za neskoršie zaplatenú faktúru, zrušenie emailového konta po nesplnení výzvy, atď.)
4. Žiadosť o zadanie osobných údajov - hlavný znak phishingového emailu. Bankové inštitúcie nikdy nežiadajú osobné informácie a prístup do konta. Online služby sa tiež často vyhýbajú žiadostiam o prihlasovacie údaje používateľa.
5. Podozrivé domény - ak vás niekto nabáda, aby ste klikli na nejaký odkaz, najprv preskúmajte URL adresu, či sa zhoduje s legitímnou stránkou.
6. Neočakávaný email - Online služby a bankové inštitúcie málokedy posielajú email žiadajúci údaje neočakávane. Príkladom neočakávanej správy je email informujúci o skoršom vydaní výpisu z účtu, ktorý si môžete vyžiadať po prihlásení sa do vášho bankového konta. Naopak očakávanou správou je reakcia na vašu činnosť, napríklad že po zmene vášho hesla, vám inštitúcie spätne pošlú informačný email o tejto skutočnosti.

Ako sa chrániť pred phishingom?

1. **Neklikajte na odkazy** v podozrivých správach. Stále si prekontrolujte URL adresu stránky. Adresa stránky, ktorá sa zobrazuje v emaili nemusí byť zhodná s tou, ktorá sa otvorí v prehliadači po kliknutí na daný odkaz. Skutočný odkaz sa zobrazí po podržaní kurzora nad adresou v emaili.
2. **Nesťahujte a neotvárajte neočakávané prílohy.** Takýmto spôsobom sa môže infikovať vaše zariadenie malvérom, napríklad ransomvérom. Obzvlášť podozrivé sú súbory, ktoré majú dve koncovky (napr. faktura.pdf.exe, upomienka.pdf.zip). Preto je dobré mať zapnuté zobrazovanie koncoviek súborov.
3. **Kontrolujte email** odosielateľa emailu. V MS Outlook sa často zobrazí len meno odosielateľa, preto je na ňom potrebné podržať kurzor, aby sa daná adresa zobrazila.
4. **Sledujte novinky** o phishingových technikách. Ak sa vyskytne nová phishingová kampaň, webové stránky venujúce sa bezpečnosti často zverejnia varovanie.
5. **Buďte ostražití voči poskytovaniu osobných údajov**. Ak vám od určitej inštitúcie prišiel neočakávaný email žiadajúci vaše údaje, overte si to radšej priamo u odosielateľa. Kontakt nájdete na jeho oficiálnej stránke. Nepoužívajte kontakt uvedený v emaili, pretože môže byť podvrhnutý.

Phishingové emaily sa dajú rozpoznať aj pomocou analýzy emailovej hlavičky.

Phishingové emaily

rozpoznanie a obrana

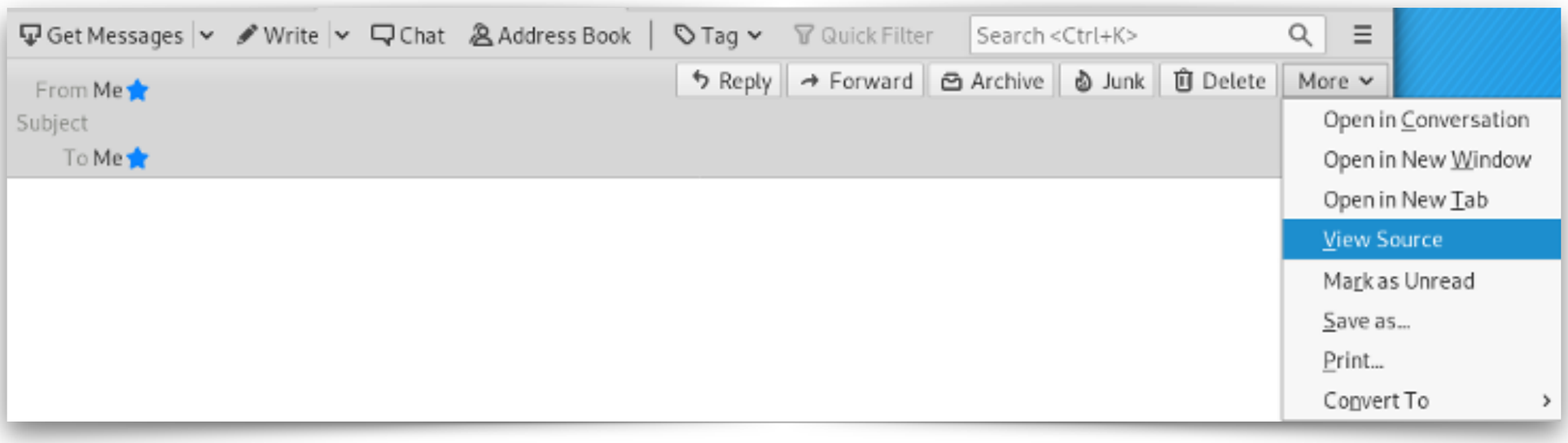
ÚRAD PODPREDSEDU VLÁDY SR PRE INVESTÍCIE A INFORMATIZÁCIU

CSIRT.SK

Ako získať e-mailové hlavičky?

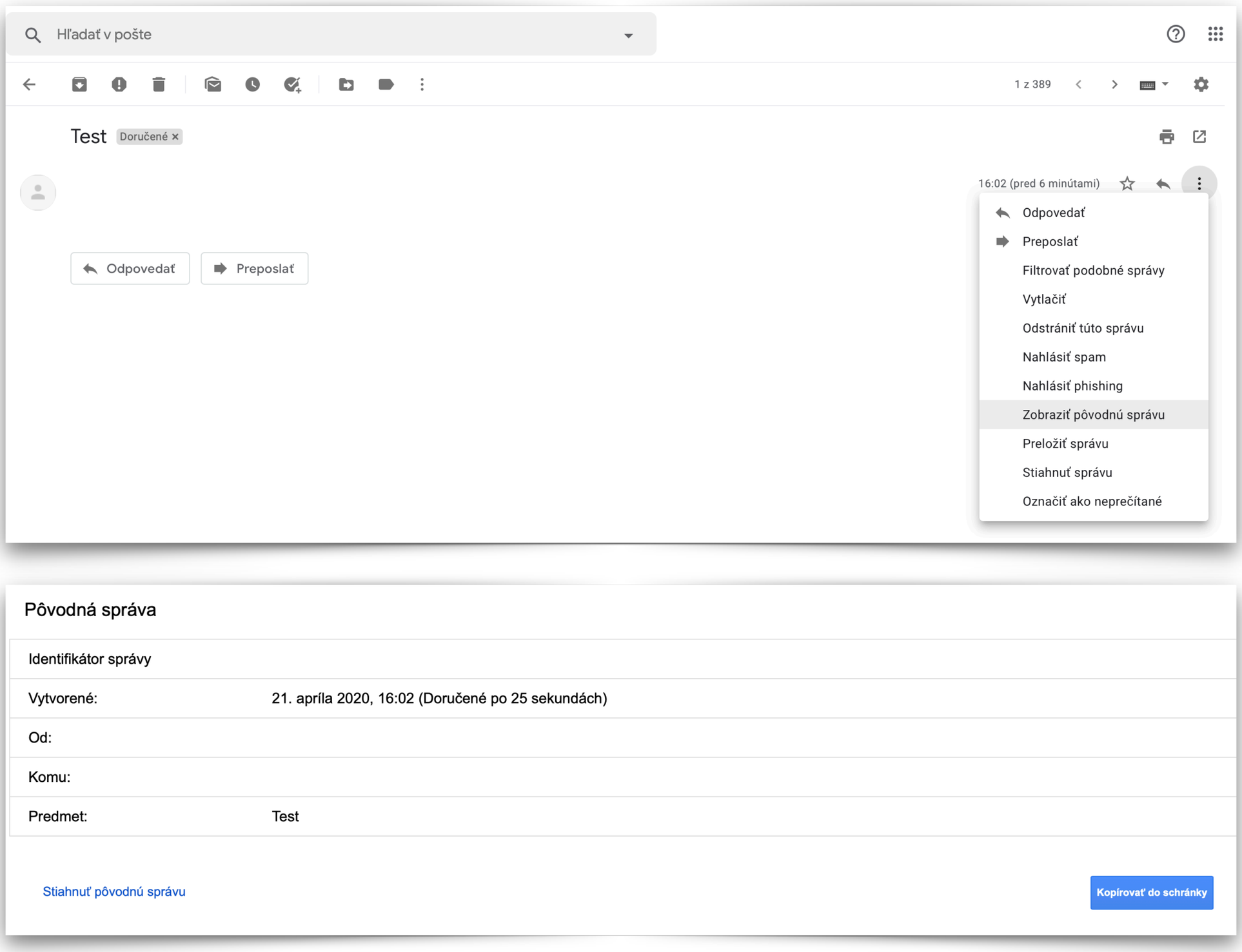
Mozilla Thunderbird

1. Dvojitým kliknutím na email sa tento otvorí v novom okne
2. V hornom menu zvoľte Ďalšie > Zobraziť zdrojový kód, otvorí sa textový súbor
3. Klávesovou skratkou Ctrl + S uložíte daný textový súbor



Gmail

1. Po otvorení daného emailu kliknete na tri bodky vpravo hore vedľa tlačidla Odpovedať
2. Zvolíte Zobraziť pôvodnú správu
3. Na stiahnutie celej správy vo formáte .eml zvoľte Stiahnuť pôvodnú správu, na stiahnutie zdrojového kódu emailu zvoľte Kopírovať do schránky a skopírovaný text si následne uložte do súboru

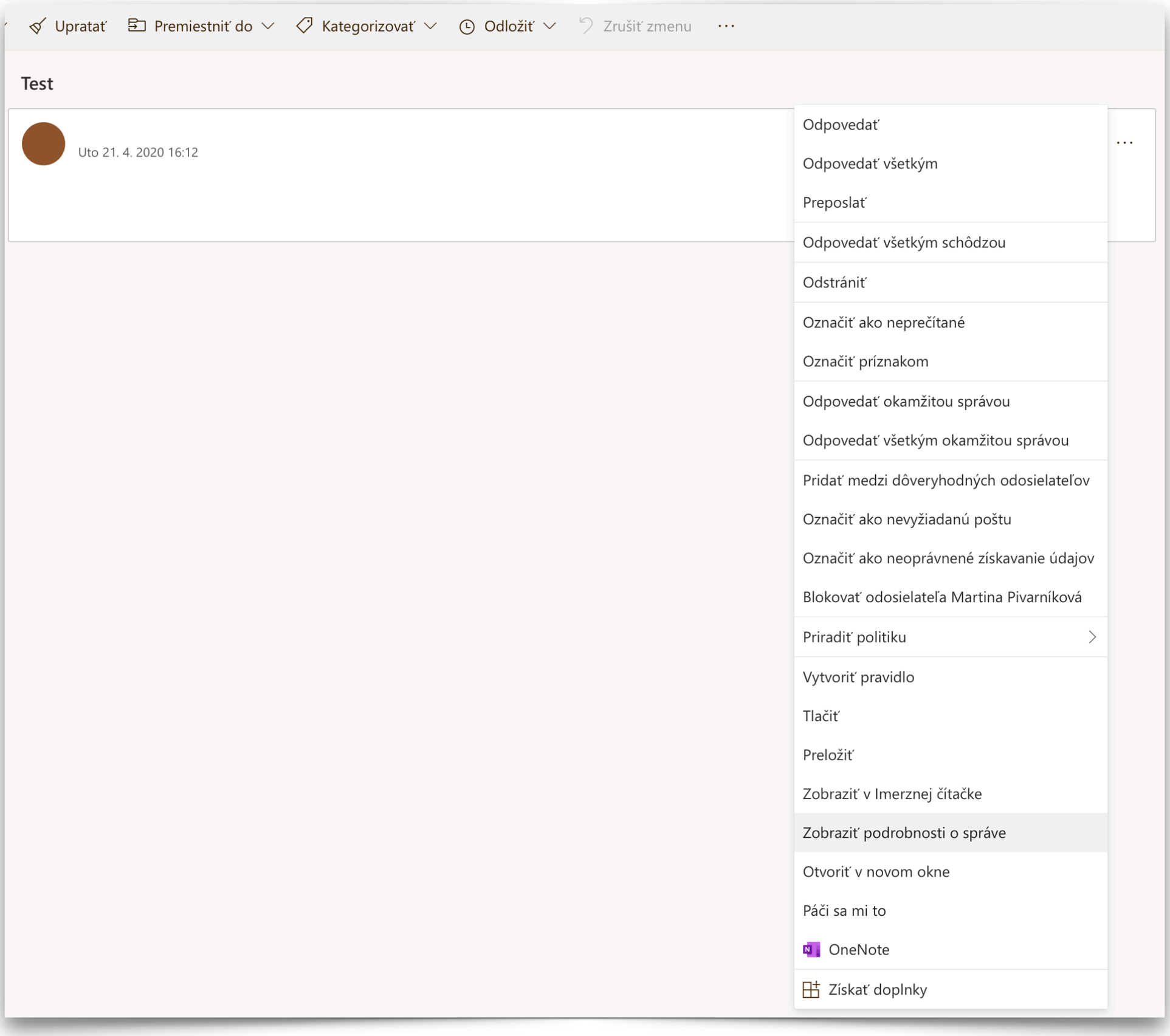


Outlook Office 365 – aplikácia

1. Po otvorení daného emailu vyberte v hornom menu panel Odoslať alebo prijať
2. Kliknite na Stiahnuť hlavičky

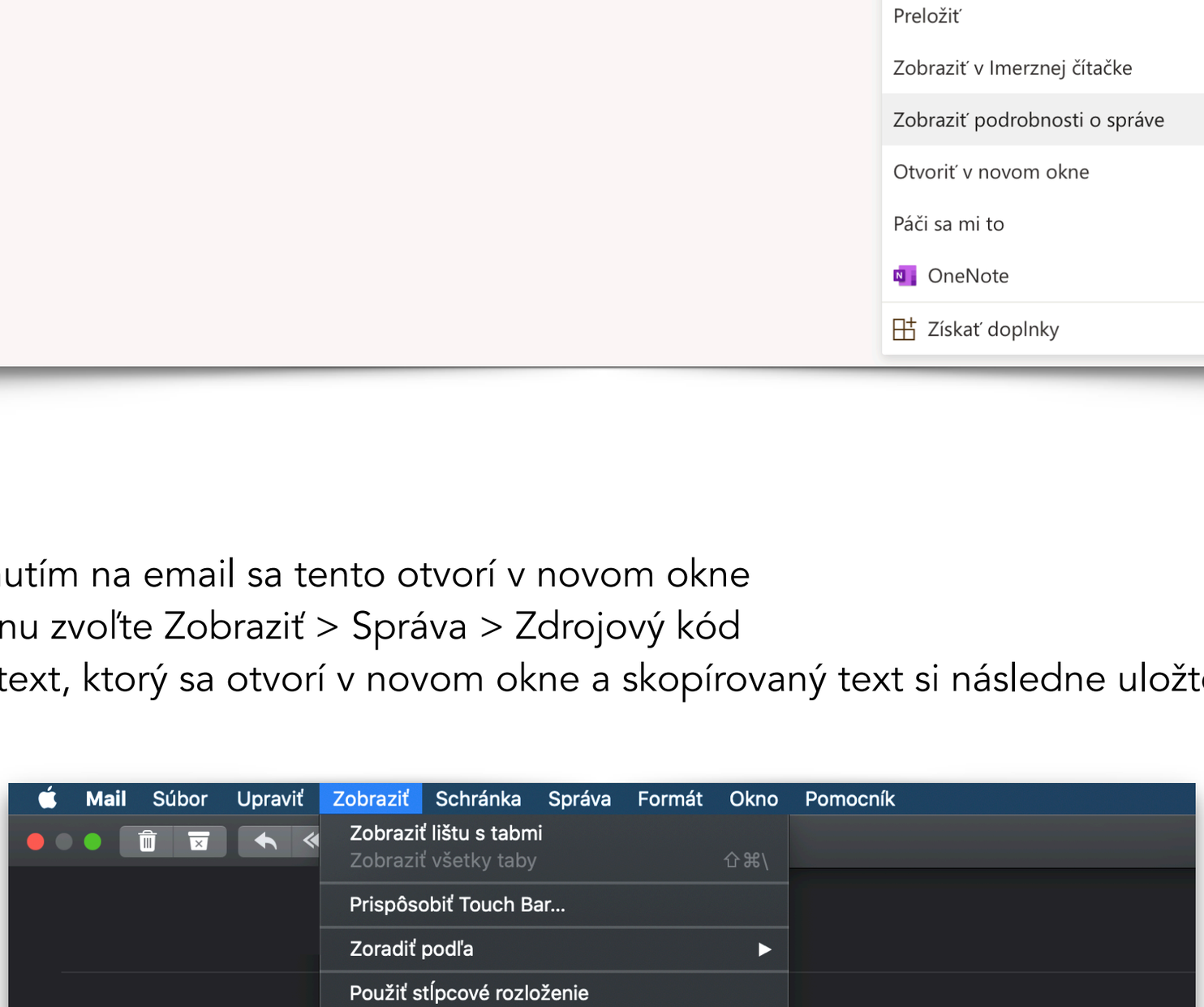
Outlook Office 365 - cez prehliadač

1. Po otvorení daného emailu kliknete na tri bodky vpravo hore vedľa tlačidla Preposlať
2. Zvoľte možnosť Zobraziť podrobnosti o správe
3. Označte celý text, ktorý sa otvorí v novom okne a skopírovaný text si následne uložte do súboru



Apple Mail

1. Dvojitým kliknutím na email sa tento otvorí v novom okne
2. V hornom menu zvoľte Zobraziť > Správa > Zdrojový kód
3. Označte celý text, ktorý sa otvorí v novom okne a skopírovaný text si následne uložte do súboru



Online nástroje na analýzu e-mailovej hlavičky:

- MX Toolbox Email Header Analyzer
- ipTRACKERonline
- DNS Checker
- Message Header Analyzer
- WhatIsMyIP Email Header Analyzer

a mnoho ďalších.

Čo z hlavičky môžeme získať?

Nasledujúca e-mailová hlavička pochádza z e-mailového klienta Outlook 365.

Received [1] : from XXX.eurprd06.prod.outlook.com (2603:10a6:207:8::20)
by XXX.eurprd06.prod.outlook.com with HTTPS via
XXX.EURPRD07.PROD.OUTLOOK.COM; Thu, 8 Feb 2018 22:40:43 +0000
Authentication-Results [2] : user.domain.sk;
dkim=none (message not signed)
header.d=none;
student.upjs.sk;
dmarc=none action=none
header.from=user.domain.sk;
Received: from YYY.eurprd06.prod.outlook.com (52.134.73.12) by
YYY.eurprd06.prod.outlook.com (52.134.66.33) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256) id
15.20.464.11; Thu, 8 Feb 2018 22:40:42 +0000
Received: from YYY.eurprd06.prod.outlook.com
([MAC ADDRESS]) by YYY.eurprd06.prod.outlook.com
([MAC ADDRESS]) with mapi id Z.Z.Z.Z; Thu, 8 Feb 2018
22:40:41 +0000
Content-Type [3] : application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding [4] : binary
From: <user1@mail.sk>
To: <user2@mail.sk>, <user3@mail.sk>
CC [5] : <user4@mail.sk>
Subject [6] :
Thread-Topic:
Thread-Index [7] :
Date: Thu, 8 Feb 2018 22:40:41 +0000

---

1 Toto pole sa objavuje ak správa bola interne prenesená medzi rôznymi servermi patriacimi k tej istej dôveryhodnej ADMD (Administrative Management Domain), administratívnej riadiacej doméne.
2 Táto časť hlavičky je definovaná štandardom RFC 8601. Sprostredkúva výsledky rôznych kontrol autentifikácie správ. DKIM (DomainKeys Identified Mail) kontroluje obsah správy využívajúc digitálne podpisy. DMARC (Domain-based Message Authentication, Reporting & Conformance) špecifikuje politiku pre autentifikované správy, je postavený na SPF (Sender Policy Framework) a DKIM.
3 Táto časť hlavičky je definovaná štandardom RFC 1049. Popisuje typ prílohy, tento konkrétny riadok znamená, že správa obsahuje ako prílohu aplikáciu a to súbor „winmail.dat“. Tento súbor obsahuje informácie pre formátovanie správ. Táto príloha sa vytvára ak je správa odoslaná z klienta Microsoft Outlook, ktorý je nesprávne nakonfigurovaný. Content-Type môže nadobúdať hodnoty text, multipart, message, image, audio, video a application.
4 Pole špecifikuje pomocné kódovanie ktoré sa použilo na údaje v správe, aby im bolo umožnené prejsť prenosnými mechanizmami, ktoré obsahujú obmedzenia znakovej sady.
5 V preklade Carbon Copy, určuje príjemcov, ktorým má byť odoslaná kópia správy. Ak správa obsahuje BCC, znamená to, že má Blind CC príjemcov, teda príjemcov skrytých pre ostatných príjemcov.
6 Popisuje predmet správy.
7 Popisujú detaily vlákna správ, teda pravdepodobne sa jedná o správu, ktorá bola odpoveďou na inú.

Message-ID: <ID@domain.sk>
References [8] : <xyz@id.eurprd06.prod.outlook.com>
<abc@id.eurprd06.prod.outlook.com>
In-Reply-To: <abc@id.eurprd06.prod.outlook.com>
Accept-Language: sk-SK, en-US
Content-Language: sk-SK
X-MS-Has-Attach [9] : yes
X-MS-Exchange-Organization-SCL [10] : -1
X-MS-TNEF-Correlator [11] : < id@domain.sk>
MIME-Version [12] : 1.0
X-MS-Exchange-Organization-MessageDirectionality: Originating
X-MS-Exchange-Organization-AuthSource: id.eurprd06.prod.outlook.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP [13] : [X.X.X.X]
X-MS-Exchange-Organization-Network-Message-Id:
X-MS-PublicTrafficType: Email
X-Microsoft-Exchange-Diagnostics: ...
X-MS-Exchange-Antispam-SRFA-Diagnostics: SSOS;SSOR;
X-MS-Exchange-Organization-AVStamp-Service: 1.0
Return-Path [14] : user1@mail.sk
X-MS-Office365-Filtering-Correlation-Id: 2b98c318-ae9a-4570-0746-08d56f44fbc1
X-Microsoft-Antispam:
X-Microsoft-Exchange-Diagnostics: ...
X-MS-TrafficTypeDiagnostic:
X-Exchange-Antispam-Report-Test: UriScan:()()();
X-Exchange-Antispam-Report-CFA-Test:
X-Microsoft-Exchange-Diagnostics: ...
X-Forefront-Antispam-Report:
X-Microsoft-Exchange-Diagnostics: ...
SpamDiagnosticOutput: 1:0
X-Microsoft-Exchange-Diagnostics: ...
X-MS-Exchange-Inbox-Rules-Loop: user3@mail.sk
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 08 Feb 2018 22:40:41.2640 (UTC)
X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id:
X-MS-Exchange-CrossTenant-Network-Message-Id:
X-MS-Exchange-Transport-CrossTenantHeadersStamped: id
X-MS-Exchange-Transport-EndToEndLatency: 00:00:02.1245582
X-MS-Exchange-Processed-By-BccFoldering:
X-Microsoft-Exchange-Diagnostics:
X-Microsoft-Antispam-Message-Info:
X-Microsoft-Exchange-Diagnostics:
...

8 Obsahuje referencie na príjemcov, jedna z týchto hodnôt sa zhoduje s nasledujúcim poľom In-Reply-To.
9 Odpovedá na otázku, či správa obsahuje prílohu. Všetky polia v hlavičke začínajúce X-MS, sú rozširujúce polia generované klientom Microsoft Exchange (Outlook 365).
10 Hodnotí Spam confidence level, teda spam skóre, generované zvyčajne e-mailovým klientom prijímateľa.
11 TNEF (Transport Neutral Encapsulation Format) je formát e-mailovej prílohy, ktorý používajú Microsoft Outlook a Microsoft Exchange Server.
12 MIME (Multipurpose Internet Mail Extension) je internetový štandard, ktorý rozširuje základný formát emailu.
13 Určuje pôvodnú IP adresu klienta, ktorý sa pripája k HTTP rozhraniu poštovej služby.
14 Môže označovať rovnakého používateľa ako Reply-To.