

- Laboratorul 4 - *Phishing*

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători!**

1. Noțiuni generale



Atribuiți fiecărui termen definiția corespunzătoare. Definițiile au fost preluate din glosarul de termeni *NIST – Computer Security Resource Center* [1]. Puteți citi mai multe despre *phishing* în documentul *European Union Agency for Cybersecurity* (ENISA) dedicat acestui subiect [2].

(A) Inginerie socială

(B) Phishing

(C) Whaling

(D) Pharming

(E) Spear phishing

(F) Spoofing

(1) Un tip specific de phishing care vizează membrii de rang înalt ai organizațiilor.

(2) O tehnică pentru încercarea de a achiziționa date sensibile, cum ar fi numerele de cont bancar, printr-o solicitare frauduloasă prin e-mail sau pe un site web, în care făptuitorul se maschează ca o afacere legitimă sau o persoană de încredere.

(3) Utilizarea mijloacelor tehnice pentru a redirecționa utilizatorii către accesarea unui site Web fals, mascat drept unul legitim și divulgarea informațiilor personale.

(4) O încercare de a păcăli pe cineva să dezvăluie informații (de exemplu, o parolă) care pot fi folosite pentru a ataca sisteme sau rețele.

(5) Falsificarea adresei de trimitere a unei transmisii pentru a obține intrarea ilegală într-un sistem securizat.

(6) Un termen colocvial care poate fi folosit pentru a descrie orice atac de phishing foarte vizat.

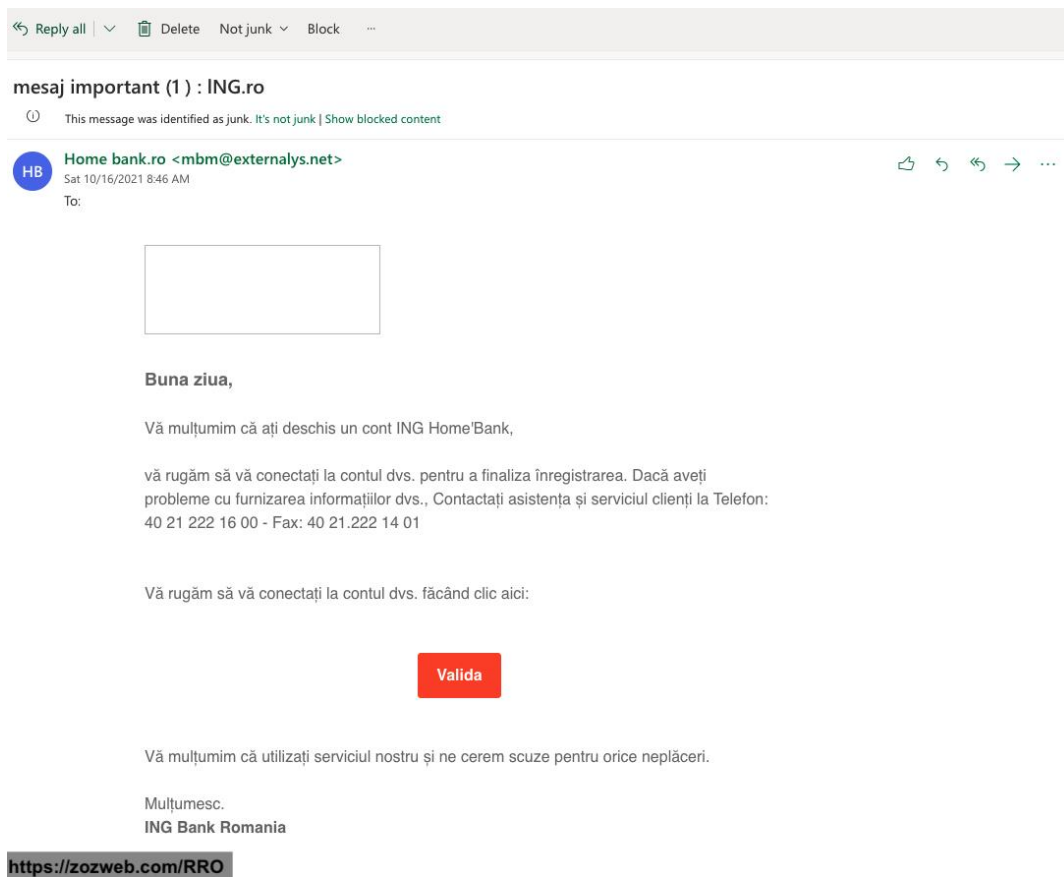
2. Identificarea vizuală a unui atac de tip phishing



Vizualizați video-ul [3].



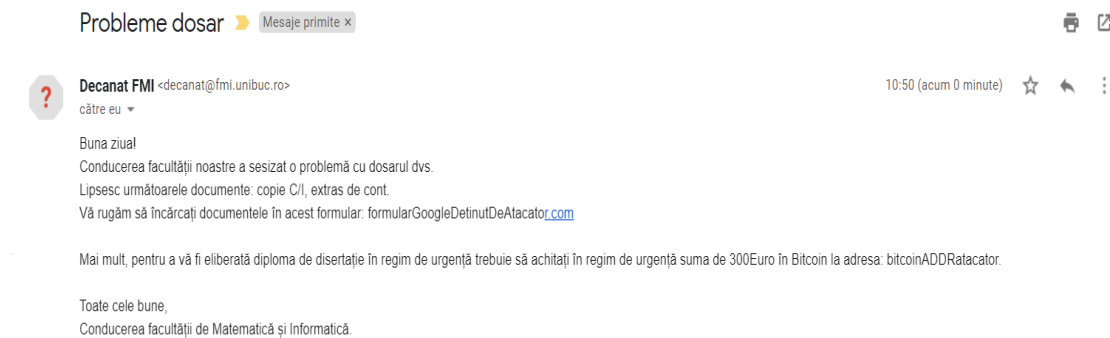
Analizați mesajul din figura de mai jos. Indicați cel puțin 3 elemente care vă indică faptul că este vorba despre un mesaj de phishing.



3. Analiza e-mailurilor de tip phishing



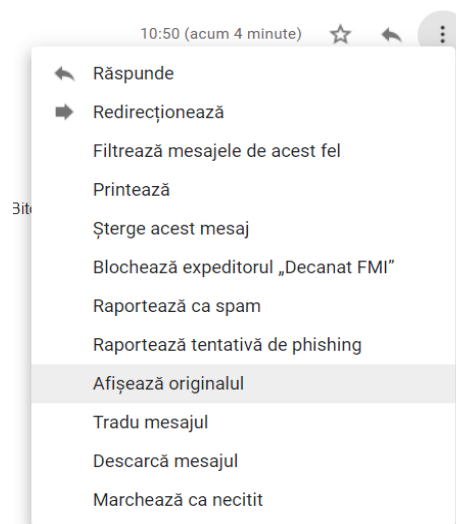
Citiți despre SPF, DKIM, DMARC online [4]. Analizați e-mailul următor:



Informațiile afișate sunt următoarele:

de la: **Decanat FMI** <decanat@fmi.unibuc.ro>
răspunde la: decanat@fmi.unibuc.ro
cătore:
data: 20 aug. 2021, 10:50
subiect: Probleme dosar
securitate: Criptare standard (TLS) [Află mai multe](#)
 : Important în opinia Google

În Gmail, folosit pentru acest exemplu, în dreptul opțiunii *Răspunde (Reply)*, la click pe *Mai multe (More)*, apăsați pe *Afișează originalul (Show original)*



Folosiți tool-uri precum [5,6] pentru a analiza header-ul și tool-uri precum [7] pentru a determina domeniul unui IP. Pentru exemplul de mai sus, câteva rezultate care indică phishing-ul sunt evidențiate în figurile următoare:

Received headers					
Hop1	Submitting host	Receiving host	Time	Delay	Type →
1		emkei.cz (Postfix, from user: 33)	8/20/2021 10:50:24 AM		
2	emkei.cz (emkei.cz. [101.99.94.155])	mx.google.com	8/20/2021 10:50:25 AM	1 second	ESMTPS
3		2002:a05:6a10:4410:0:0:0	8/20/2021 10:50:26 AM	1 second	SMTP

101.99.94.155 - Geo Information	
IP Address	101.99.94.155
Host	emkei.cz
Location	MY, Malaysia
City	*,
Organization	Piradius Net
ISP	Piradius Net

Received-SPF	softfail (google.com: domain of transitioning decanat@fmi.unibuc.ro does not designate 101.99.94.155 as permitted sender) client-ip=101.99.94.155;
Authentication-Results	mx.google.com: spf=softfail (google.com: domain of transitioning decanat@fmi.unibuc.ro does not designate 101.99.94.155 as permitted sender) smtp.mailfrom=decanat@fmi.unibuc.ro; dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=unibuc.ro

Atenție! Nu abuzați de astfel de unelte și nu le folosiți în scopuri rău intenționate! Nu trimiteți un email de pe acest site altcuiva, ci doar către adresa de email personală, în scopul exclusiv de a învăța! Revedeți disclaimer-ul de la începutul fiecărui laborator.

Referințe bibliografice

1. National Institute of Standards and Technology (NIST) – Computer Security Resource Center (CSRC), *Glossary*. Accesibil la: <https://csrc.nist.gov/glossary/>
2. ENISA. ENISA, *Threat Landscape 2020 – Phishing*. Accesibil la: <https://www.enisa.europa.eu/publications/phishing>.
3. IDG TECHtalk, *What is phishing? Learn how this attack works*. Accesibil la: https://www.youtube.com/watch?v=Y7zNIEMDmI4&ab_channel=IDGTECHtalk
4. CSO Online. *What are DMARC, SPF and DKIM? How to master email security with these protocols*. Accesibil la: <https://www.csoonline.com/article/3254234/mastering-email-security-with-dmarc-spf-and-dkim.html>.
5. *Message Header Analyzer*. Accesibil la: <https://mha.azurewebsites.net/>
6. Google Admin Toolbox. *Messageheader*. Accesibil la: <https://toolbox.googleapps.com/apps/messageheader/>.
7. Da whois. IP Address / Domain Name Lookup. Accesibil la: <https://dawhois.com/>