PHISHING

Ghid de conștientizare a atacurilor cibernetice de tip PHISHING asupra serviciilor publice utilizate în INTERNET

CUPRINS

Ce este Phishing-ul? - Definiție

Phishing-ul (**fraudă electronică**) este un tip de atac cibernetic ce are ca scop obținerea accesului la informații. Prin intermediul phishing-ului, persoanele rău intenționate crează și trimit e-mailuri frauduloase, mesaje text, apeluri telefonice sau folosesc site-uri web pentru a manipula utilizatorii să ofere acces la informații sensibile și date confidențiale sau să descarce programe *malware*[1] pe dispozitive.

Etapele unui atac de tip phishing

Acțiunea unui atac de tip phishing poate fi descrisă astfel:

1. Identificarea țintei: reprezintă procesul prin care persoanele rău intenționate selectează utilizatorii sau structurile pe care intenționează să le exploateze, analizând informații disponibile public, comportamente online sau vulnerabilități specifice.

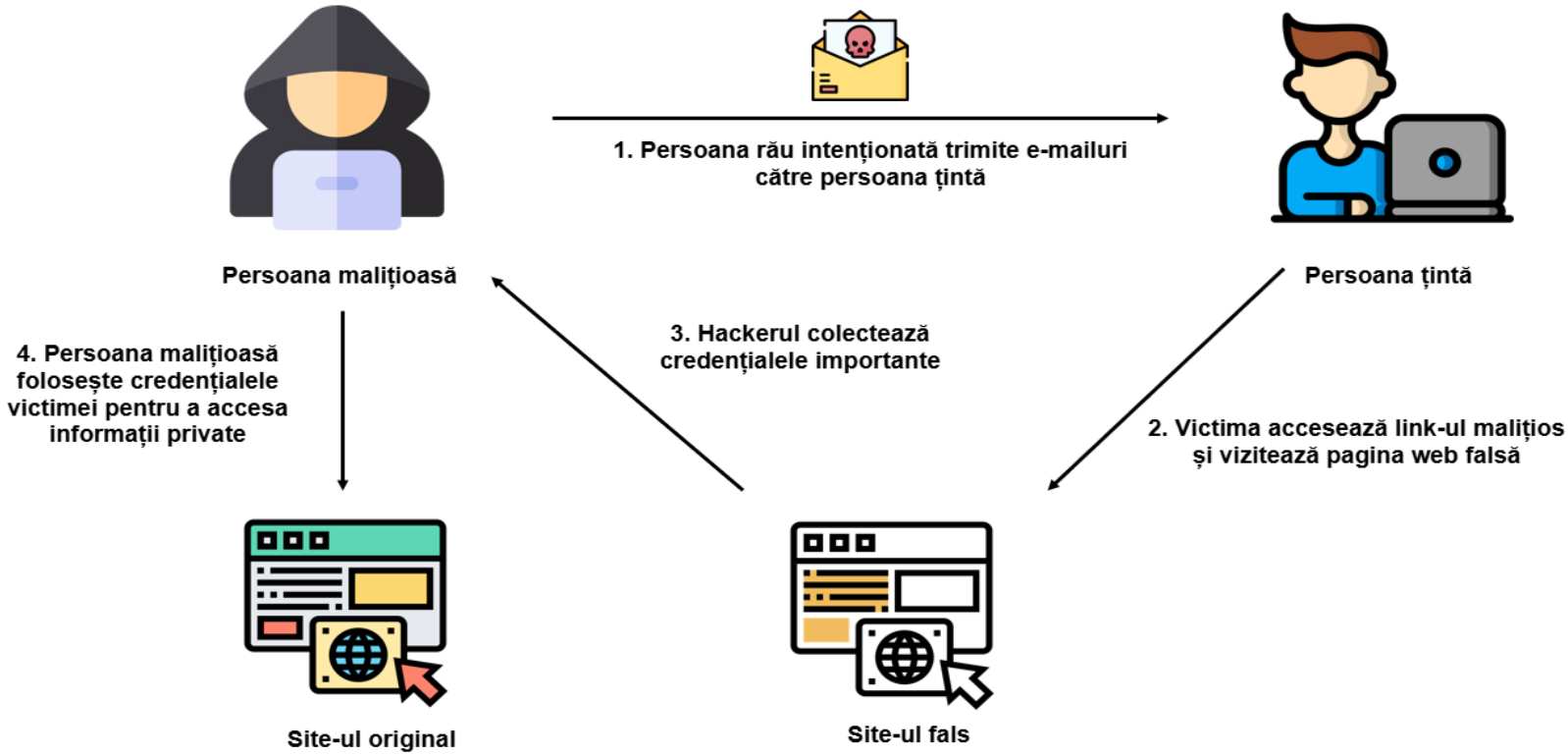
2. Crearea vectorului de atac: constă în proiectarea și pregătirea mijloacelor prin care persoana rău intenționată va păcăli utilizatorul pentru a obține informații sensibile sau acces neautorizat la date.

[1] Software rău intenționat, dăunător, ce a fost creat cu scopul de a deteriora un computer, un server sau o rețea de internet (ex. viruși, viermi, trojan, ransomware sau spyware).

3. Lansarea atacului: trimiterea de mesaje malițioase către victimele vizate, folosind canale de comunicare precum e-mailuri, mesaje SMS, rețele sociale sau alte platforme online.

4. Exploatarea erorii umane: se bazează pe manipularea victimei cu scopul de a o determina să comită o greșeală, cum ar fi furnizarea de informații sensibile sau accesarea unui link malițios.

5. Compromiterea datelor: persoana rău intenționată obține informațiile sensibile ale victimei, cum ar fi credențiale, date financiare, informații cu caracter personal, prin intermediul unui mesaj fals.



Cum recunoști un atac de tip phishing

Pentru a identifica un atac de phishing, trebuie urmărite câteva semne și comportamente comune care pot indica o tentativă de înșelăciune:

***1. Verificarea expeditorului**:* Adresele de e-mail sau numele expeditorilor pot părea suspecte. De obicei, persoanele rău intenționate folosesc adrese care sunt foarte asemănătoare cu cele legitime, dar pot conține mici diferențe (exemplu: „ion.po**pp**escu@ma**pp**n.ro” în loc de „ion.popescu@mapn.ro”).

***2. Mesaje cu erori gramaticale sau de ortografie**:* Multe atacuri de phishing conțin greșeli de ortografie, care sunt un indiciu că mesajul nu provine de la o sursă oficială.

***3. Solicitări urgente sau amenințări**:* Persoanele rău intenționate încearcă adesea să creeze o situație de urgență sau un sentiment de panică, cu precizarea că este necesară o acțiune imediată din partea utilizatorului pentru evitarea pierderii de date sau blocării contului (ex. „Contul tău va fi blocat dacă nu îți actualizezi informațiile acum!”).

***4. Link-uri suspecte**:* Verificați URL-urile din mesaje. Chiar dacă adresa URL pare corectă, în realitate poate fi diferită. Pentru verificare poziționați cursorul peste link fără a-l accesa pentru a

vedea adresa completă. Site-urile oficiale vor utiliza adrese sigure (ex. „https://”), iar URL-urile suspecte pot include caractere neobișnuite sau diferite de cele oficiale.

5. Solicitări de informații sensibile: Dacă primiți mesaje în care vă sunt solicitate date cu caracter personal (parole, numere de card, informații bancare) acestea sunt un semn al atacurilor de phishing. Structurile legitime nu vor cere astfel de informații prin aceste mijloace.

6. Fișiere atașate malițioase sau suspecte*:* Deschiderea unui fișier de la un expeditor necunoscut poate duce la infectarea dispozitivului cu programe malware. Acordați o atenție sporită fișierelor de tip .exe, .zip, sau alte formate neobișnuite în cadrul e-mail-urilor.

7. Verificarea sursei*:* Dacă aveți îndoieli, contactați direct structurile din partea cărora pare că provine mesajul, folosind datele de contact oficiale cunoscute. Nu răspundeți niciodată direct la mesajele suspecte și nu folosiți informațiile de contact din mesajul respectiv.

Tehnici frecvent utilizate în phishing

Phishing-ul este una dintre cele mai răspândite și periculoase forme de atac cibernetic bazate pe inginerie socială, adaptându-se constant la diferite medii de comunicare pentru a înșela utilizatorii și a obține date sensibile.

1. E-mail Phishing

Aceasta este cea mai comună formă de phishing, unde atacatorii trimit e-mailuri frauduloase ce par a proveni de la structuri de încredere (bănci, platforme de plăți, companii cunoscute). Scopul este de a convinge victima să acceseze un link malițios, să descarce un fișier infectat sau să furnizeze date confidențiale.

2. Smishing (Phishing prin SMS și mesaje mobile)

Smishing-ul folosește mesaje text pentru a înșela utilizatorii să acceseze link-uri periculoase sau să divulge informații personale. Aceste mesaje par a veni de la structuri bancare, structuri de logistică sau structuri importante și exploatează sentimente de urgență pentru a forța victima să reacționeze rapid.

3. Vishing (Phishing prin apeluri telefonice)

Atacatorii folosesc apeluri telefonice pentru a se prezenta drept reprezentanți ai unor structuri de încredere, încercând să obțină date bancare, parole sau coduri de autentificare. Uneori, folosesc tehnologii de falsificare a identității apelantului (caller ID spoofing) pentru a părea credibili.

4. Spear Phishing (Phishing direcționat/țintit)

Un atac personalizat care vizează o anumită persoană sau structură. Atacatorii colectează informații despre țintă din surse publice și creează mesaje convingătoare ce par să provină de la colegi de serviciu sau superiori.

5. Whaling (Phishing asupra persoanelor cu funcții superioare)

O formă avansată de spear phishing, care vizează personalul de comandă și factori de decizie ai unei structuri. Scopul este obținerea de informații confidențiale sau deturnarea fondurilor. Atacatorii cercetează atent persoana țintă folosind surse publice, precum rețelele sociale.

6. Clone Phishing (Phishing prin e-mailuri clonate)

Atacatorii copiază un e-mail legitim primit anterior, modificând conținutul pentru a introduce link-uri malițioase sau fișiere infectate. Deoarece mesajul pare autentic, victimele sunt mai predispuse să cadă în capcană.

7. Angler Phishing (Phishing prin rețele sociale)

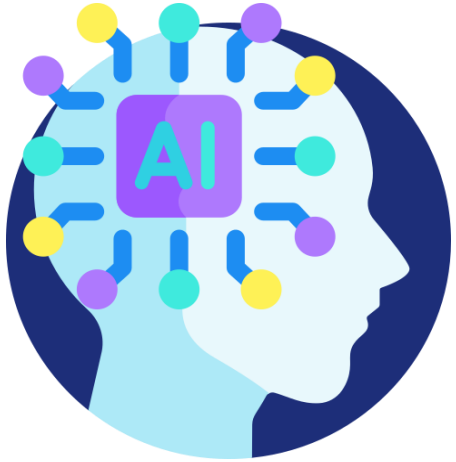
Atacatorii folosesc conturi false, mesaje frauduloase sau răspunsuri înșelătoare pe rețelele sociale pentru a obține informații personale sau acces la conturile utilizatorilor. Acest tip de atac exploatează încrederea oamenilor în branduri, servicii sau persoane cunoscute.

Phishing și inteligența artificială – O evoluție periculoasă

Pe măsură ce tehnologia avansează, atacatorii cibernetici folosesc noi mecanisme precum **Inteligența Artificială (AI)** pentru a îmbunătăți tehnicile de phishing, făcându-le mai complexe, mai greu de detectat și mai eficiente. AI permite atacatorilor să personalizeze atacurile, să automatizeze procesele și să creeze conținut convingător, eliminând greșelile de gramatică sau ortografie cât mai eficient.

1. Generarea de mesaje de phishing mai realiste și mai convingătoare

Atacatorii folosesc *modele de limbaj AI* (precum ChatGPT, Gemini, Claude) pentru a genera e-mailuri, mesaje SMS și postări pe rețele sociale fără greșeli gramaticale și cu un ton profesional sau prietenos, în funcție de context. AI poate analiza și adapta mesajele pentru a le face mai credibile și mai personalizate.



2. Phishing personalizat prin analiza Big Data și Social Engineering

AI poate analiza cantități uriașe de date (Big Data) colectate de pe *rețele sociale, site-uri web și baze de date publice* pentru a crea atacuri extrem de personalizate (ca de exemplu: spear phishing).

3. Deepfake Phishing – Folosirea AI pentru a falsifica voci și videoclipuri

Tehnologia *deepfake* reprezintă crearea de *clipuri video și audio false* care imită perfect vocea sau imaginea unei persoane folosind AI. Astfel, victimele sunt păcălite să creadă că interacționează cu o persoană reală.

4. Automatizarea atacurilor de phishing la scară largă

AI permite *automatizarea și scalarea atacurilor de phishing*, în acest mod atacatorii pot să trimită milioane de e-mailuri, mesaje și notificări personalizate într-un timp foarte scurt.

5. Bypass-ul filtrelor anti-phishing cu ajutorul AI

Multe sisteme de securitate cibernetică folosesc filtre bazate pe reguli pentru a detecta și bloca mesajele de phishing. Atacatorii folosesc AI pentru a optimiza mesajele astfel încât să evite detectarea.

6. Phishing prin atacuri asupra dispozitivelor Internet of Things (IoT [2]) și asistenților virtuali

Atacatorii folosesc AI pentru a crea *comenzi vocale malițioase* sau pentru a intercepta comunicațiile dispozitivelor IoT și ale asistenților vocali, cum ar fi Alexa, Siri sau Google Assistant.

7. Phishing prin platforme de colaborare (SaaS Phishing)

Pe măsură ce tot mai multe companii folosesc *platforme SaaS* (Software-as-a-Service) precum Google Drive, Microsoft Teams, Slack, Trello, atacatorii trimit invitații sau notificări false care par să provină de la aceste platforme și redirecționează utilizatorii către pagini de phishing.

8. Phishing prin cod QR (Quishing – QR Code Phishing)

Atacatorii înlocuiesc link-urile de phishing obișnuite cu *coduri QR malițioase*, care sunt plasate în e-mailuri, postere, reclame sau chiar în locuri fizice, cum ar fi restaurante și benzinării. Când utilizatorul scanează codul QR, acesta este redirecționat către un site fals, unde îi sunt solicitatedate personale sau date de autentificare.

[2] Echipamente conectate la internet, capabile să colecteze, trimită și primească date fără intervenția directă a utilizatorului (senzori, electrocasnice inteligente, camere de supraveghere, ceasuri smart etc.).

Cum prevenim atacurile de phishing – Măsuri de protecție

1. Utilizarea autentificării multi-factor (MFA)

Importanța utilizării Autentificării Multi-factor (MFA) constă în creșterea securității conturilor și a datelor prin adăugarea unui nivel suplimentar de verificare, pe lângă parolă. MFA reduce riscul de acces neautorizat chiar dacă parola a fost compromisă, solicitând utilizatorului să furnizeze o a doua formă de autentificare, cum ar fi un cod generat pe telefon, o amprentă digitală sau un token hardware.

2. Filtrarea și blocarea e-mailurilor

Necesitatea filtrării și blocării e-mailurilor de phishing se bazează pe prevenirea accesului utilizatorilor la mesaje malițioase care încearcă să colecteze date sensibile, cum ar fi parole, informații financiare sau detalii personale. Prin implementarea de filtre avansate anti-phishing și tehnologii precum SPF, DKIM și DMARC, structurile pot detecta și bloca e-mailurile frauduloase înainte ca acestea să ajungă în inbox-ul utilizatorilor.

Majoritatea serviciilor moderne de e-mail, inclusiv cele accesate prin aplicații de pe Android și iOS, dispun de sisteme automate de filtrare a mesajelor. Acestea folosesc inteligență artificială și liste negre (blacklist[3]) actualizate constant pentru a identifica e-mailurile suspecte și a le muta automat în dosarul "Spam" sau "Junk", reducând semnificativ riscul ca utilizatorii să acceseze

[3] Mecanism de securitate care blochează accesul anumitor adrese IP, domenii, e-mailuri sau aplicații considerate periculoase.

conținut periculos. De asemenea, utilizatorii pot marca manual e-mailurile ca fiind phishing, contribuind astfel la îmbunătățirea acestor filtre.

3. Evitarea introducerii de date cu caracter sensibil

Importanța evitării introducerii de date cu caracter sensibil pe site-uri necunoscute constă în protejarea informațiilor personale și financiare împotriva furtului și utilizării frauduloase. Site-urile necunoscute sau nesecurizate pot fi create de persoane rău intenționate pentru a colecta date prin tehnici de phishing sau alte metode malițioase. Verificați autenticitatea unui site, folosirea conexiunilor securizate (**HTTPS**) și evitați accesarea link-urilor suspecte.

4. Verificarea surselor de comunicare

Importanța verificării surselor de comunicare se bazează pe prevenirea fraudelor, atacurilor de phishing și accesului neautorizat la informații sensibile prin confirmarea autenticității expeditorilor și a mesajelor primite. Atacatorii pot falsifica e-mailuri, mesaje sau apeluri telefonice pentru a induce în eroare victimele și a le determina să furnizeze date confidențiale sau să efectueze acțiuni malițioase.

5. Educația și conștientizarea utilizatorilor

Importanța educației și conștientizării utilizatorilor constă în reducerea riscurilor de securitate cibernetică prin instruirea acestora să recunoască și să evite amenințările, cum ar fi phishing-ul, malware-ul sau alte atacuri de inginerie socială. Transmiterea de informări interne către utilizatori pot preveni producerea eventualelor incidente de securitate cibernetică.

Mitigarea riscurilor – Cum răspundem la un atac de tip phishing

1. Izolarea și raportarea atacului

Opriți răspândirea atacului în vederea limitării impactului asupra structurii. Raportarea rapidă permite aplicarea contramăsurilor și prevenirea unor atacuri similare.

2. Resetarea credențialelor și verificarea activității contului

Puteți preveni accesul neautorizat prin schimbarea parolelor și activarea autentificării multi-factor (MFA). Verificarea activității conturilor ajută la identificarea accesărilor suspecte sau chiar neautorizate.

3. Scanarea dispozitivelor pentru amenințări

Detectați și eliminați malware-ul care ar putea compromite sistemul. Scanarea regulată cu un antivirus actualizat vă protejează datele și previne infectările.

4. Implementarea unui blacklist și a regulilor de blocare

Restricționați accesul la surse malițioase cunoscute, reducând riscul de phishing și malware. Blocați automat domenii, IP-uri și expeditori suspecți.

5. Revizuirea și îmbunătățirea măsurilor de securitate

Permiteți adaptarea la noile amenințări prin actualizarea politicilor și instrumentelor de protecție, prevenind brețele de securitate.

Referințe

- ✓ https://ro.wikipedia.org/wiki/Înșelăciune_electronică
- ✓ https://www.trendmicro.com/en_gb/what-is/phishing/types-of-phishing.html
- ✓ https://www.ncsc.gov.uk/guidance/phishing
- ✓ https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/phishing-attack-prevention.html
- ✓ https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing
- ✓ https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

Puncte de contact

În cazul în care primiți un mesaj care vă ridică suspiciuni, **evitați accesarea link-urilor sau a fișierelor atașate** și redirecționați mesajul către Centrul de Răspuns la Incidente de Securitate Cibernetică a categoriei de forțe de care aparțineți (domeniul forter.ro - CRISC SMFT, domeniul roaf.ro - CRISC SMFA, domeniul navy.ro - CRISC SMFN, domeniul mapn.ro - CRISC CCI, domeniul logmil.ro - CRISC CLI) sau către Centrul de Răspuns la Incidente de Securitate Cibernetică Principal (domeniul mapn.ro – CRISC-P) la punctele de contact afișate, iar personalul specializat va realiza o analiză a mesajului și vă va confirma sau infirma suspiciunea.

ADRESE E-MAIL DE CONTACT:

- **Centrul de Răspuns la Incidente de Securitate Cibernetică Principal:** cyber@mapn.ro
- **CRISC SMFT:** cyber@forter.ro
- **CRISC SMFA:** cyber_smfa@roaf.ro
- **CRISC SMFN:** criscfn@navy.ro
- **CRISC CCI:** cyber-CCI@mapn.ro
- **CRISC CLI:** crisc-cli@logmil.ro

AGENȚIA DE APĂRARE CIBERNETICĂ