Phishing-ul bancar
Propuneri de soluții pentru diminuarea numărului de victime ale atacurilor cibernetice de tip phishing

Oana Buzianu, Wintech, România, oana.buzianu@wintechconsulting.ro
Alexandru Ciprian Angheluș, Prodefence, contact@prodefence.ro
Gabriel Raicu, Universitatea Maritimă din Constanța, România, gabriel.raicu@cmu-edu.eu
Mircea Constantin Șcheau, Universitatea Maritimă din Constanța, România, mircea.scheau@cmu-edu.eu

1. Introducere

Odată cu extinderea semnificativă a spațiului virtual, utilizatorii din mediul online își împărtășesc din ce în ce mai multe informații personale și drept urmare, o cantitate enormă de date legate de identificare sau tranzacții financiare sunt expuse agresorilor cibernetici. Phishing-ul este unul dintre exemplele de criminalitate prin intermediul căruia infractorii își înșală victimele, cu scopul de a exploata ulterior elementele exfiltrate. De la primul atac raportat în 1990, metoda a evoluat, vectorii de livrare devenind deosebit de sofisticați. Articolul își propune evaluarea acestor acțiunii, identificarea și revizuirea tehnicilor existente.

Sectorul financiar este una dintre principale ținte ale infractorilor cibernetici, care folosesc deseori atacurile de phishing pentru a ocoli protocoalele de securitate ale băncilor, cu scopul de a-și atrage victime și de a le convinge de legitimitatea e-mailului falsificat. Aceștia apelează la diverse trucuri de inginerie socială prin crearea de scenarii (actualizare falsă a contului, upgrade de securitate etc.) și tehnici specifice (imitarea imaginilor, logo-urilor și identității instituțiilor bancare etc.).

Pentru că susceptibilitatea față de phishing variază în funcție de nivelul de conștientizare al utilizatorului, în majoritatea atacurilor infractorii cibernetici exploatează deseori natura umană, în locul utilizării tehnologiilor sofisticate. În consecință, deși protocoalele de siguranță sunt încorporate în site-urile și aplicațiile bancare, adesea elementul uman nu reușește să detecteze înșelătoria, în lipsa cunoștințelor elementare de etică digitală cu ajutorul cărora ar fi fost mai conștienți de posibilele riscuri, astfel încât intrușii să nu le fure bani și date personale sensibile.

Acest articol conține informații destul de apropiate de zona tehnică și în aceeași măsură explicații pertinente referitoare la posibile modalități de diminuare a numarului de victime expuse atacurilor.

2. Etape ale unei campanii de phishing

În etapa de inițiere a unui atac phishing, atacatorul trimite un e-mail fraudulos care se pretinde a proveni de la banca victimei solicitând destinatarului confirmarea detaliilor contului bancar, cu avertismentul că în caz de nefurnizare a informațiilor, contul poate fi suspendat. Utilizatorul poate considera email-ul ca fiind legitim, deoarece folosește aceleași elemente grafice, mărci comerciale și culori ca ale băncii reale. Datele colectate sunt transmise direct infractorului cibernetic, iar acesta le poate folosi ulterior pentru comiterea altor fraude, sau le poate revinde pe piața neagră.

Un indiciu de susceptibilitate poate fi tocmai adresa de e-mail a expeditorului, necunoscută de destinatar. Pentru că deseori mesajele de tip phishing pot include chitanțe, facturi, sau alte tipuri de documente pe care ați putea dori să le descărcați în anumite circumstanțe, vă recomandăm să fiți precauți și să luați în considerare dacă cererea are sens înainte de a descărca atașamentul și să confirmați mai întâi identitatea expeditorului. Nu este normal ca soluționarea unor probleme bancare să se facă prin intermediul unor adrese de e-mail care, cel puțin vizual, nu au legătură cu instituția, iar folosirea butonului *„Vizualizare mesaj”* să direcționeze utilizatorul către o zonă de conectare ilicită oferind atacatorilor credențialele bancare.

Din acest motiv site-urile web și fișierele din e-mail ar trebui să fie rulate în medii izolate de sistemul de operare principal (sandbox), fiind examinate posibilele modificările făcute în sistem și verificate pentru activități ascunse, de cele mai multe ori dăunătoare.

Infractorul cibernetic încearcă să inducă în eroare potențiala victimă prin utilizarea în subiectul e-mailului a sintagmei *„foarte important / urgent”*, astfel încât să declanșeze o reacție psihologică pentru a o determina să dea click pe butonul *„Vizualizare mesaj”*, un buton în spatele căruia există atașată o adresă web. La trecerea cu mouse-ul peste acest buton, sau la apăsarea timp de 3 secunde în cazul dispozitivelor mobile, apare acea adresă încorporată (de tip URL) care nu se potrivește cu adresa oficială a băncii.

Exploatarea acestei vulnerabilități umane ar putea permite unui atacator să folosească controlul DHTML Edit ActiveX (Controlul ActiveX al componentei de editare DHTML din Microsoft Windows 2000 SP4 și Windows Server 2003 SP2 nu formatează corect marcajul HTML, ceea ce permite atacatorilor de la distanță să execute cod arbitrar) încărcat de pe site-ul web rău intenționat pentru a modifica conținutul dintr-o fereastră de browser, într-un domeniu diferit. Prin urmare, verificați dacă adresa URL a site-ului începe cu „https”, indicând că site-ul este securizat cu criptare TLS/SSL. Un phisher poate păcăli un utilizator să dea click pe o adresă URL rău intenționată, care încarcă controlul DHTML Edit, deschide o nouă fereastră de browser pentru site-ul de încredere și apoi utilizează controlul vulnerabil pentru a înlocui conținutul din fereastra browserului care conține site-ul de încredere. Toate celelalte atribute ale ferestrei browser (informații despre certificatul SSL, proprietățile paginii) ar fi pentru site-ul web legitim.

Atacatorii înregistrează adesea nume de domenii care conțin numele instituției țintă pentru a înșela clienții care sunt mulțumiți că văd un nume legitim ce apare într-o adresă. O versiune implementată pe scară largă a acestui tip de atac folosește părți dintr-o adresă URL legitimă pentru a elabora un nou nume de adresă/ domeniu, foarte asemănător cu adresa oficială. Elementele din adresa de e-mail vor fi modificate astfel încât să fie suficient de asemănătoare cu o adresă de e-mail legitimă (numere adăugate, sau litere schimbate).

Majoritatea campaniilor de phishing au câteva puncte comune, ceea ce creează premisele unei construcții valide în combaterea atacurilor cibernetice și reducerea numărului de victime. Expunem în cele ce urmează câteva dintre acestea.

2.1. Folosirea resurselor băncii.

Pentru a promova o identitate falsă cât mai apropiată de cea băncii, atacatorii se folosesc uneori de resursele acesteia:

- Logo,
- Imaginea / banner-ul care apare pe prima pagină a băncii,
- Elemente ale codurilor sursă ce susțin protocoalele de acces.

GET > https://banca_preferată.ro/fișier1/fișier2/imagini/logo.png

GET > https://resurse.banca_preferată.ro/fișier1/fișier2/document.js

Figura 1. Exemple ale funcției de exploatare a resurselor
Sursă: Prodefence cyber research team

Blocarea folosirii neautorizate a resurselor unui server se poate face luând în considerație felul în care băncile relaționează cu infrastructurile externe, pentru a nu perturba buna desfășurare a activității partenerilor. Folosirea unei liste a infrastructurilor care pot accesa și utiliza resursele vizuale (sau tehnice) ale băncii are rolul de a reduce traficul de date din servere, forțând atacatorii să utilizeze în campaniile de phishing doar clone ale paginilor oficiale și ajutând implicit la alterarea credibilității paginilor false.

2.2. Vizitatorul victimă

Un alt punct comun al atacurilor de tip phishing este acela că, imediat după finalizarea colectării datelor, majoritatea paginilor false redirecționează clientul devenit victimă către paginile legitime, pentru menținerea sentimentului de siguranță al acestuia. Trebuie menționat că serverele băncilor identifică și înregistrează sursele de la care s-au conectat vizitatorii sau de la ce pagină au fost direcționați către acestea.

http(s)://pagină_falsă.x/fișier.php
Ex. final.php , sendsms.php, redirect.php, sms.php, sms2.php .. etc.

Figura 2. Exemplu fișiere de redirecționare

Sursă: Prodefence cyber research team

Dacă mai mulți clienți ajung pe pagina băncii de la o astfel de sursă comună, ar trebui să se declanșeze un mecanism (red flag) care să permită alertarea departamentului de securitate al băncii, să atenționeze clientul că există posibilitatea să fi fost ținta unui atac cibernetic și să-l sfătuiască pe acesta să ia legătura cu banca pentru blocarea cardului, verificarea aplicației de plăți online, etc.

Figura 3. Exemplu de pagină avertizare
Sursă: Prodefence cyber research team

De asemenea, se recomandă colaborarea cu resurse externe de dezvăluire a atacurilor cibernetice și a paginilor de phishing, astfel ca prin intermediul unei API (Application Platform Interface) paginile suspecte să fie incluse în lista surselor de trafic cu potențial malițios.

Această metodă va reduce semnificativ numărul victimelor, deoarece clienții vor fi avertizați în timp util de faptul că au ajuns pe pagina băncii după ce au accesat o pagină falsă, iar în cazul în care au fost convinși să introducă datele bancare vor comunica imediat instituției bancare pentru a primi sprijin din partea acesteia.

2.3. Impersonarea clientului (impersonating = imitarea/ falsificarea identității)

Gradul de succes al unui atac clasic de tip phishing se bazează destul de mult pe naivitatea clienților și are ca scop obținerea credențialelor, dar fără a exista garanția accesului la conturile bancare și implicit transferul sumelor de bani existenți. Obstacolele întâmpinate sunt reprezentate de dificultatea accesării conturilor furate, datorită sistemelor de securitate și a procedurilor implementate de instituțiile bancare pentru autorizarea clientului.

Factorii de rezistență (educație, proceduri, tehnologii) împotriva atacurilor cibernetice conduc infractorii spre elaborarea unor noi metode și tehnologii de atac. Una dintre aceste metode este încercarea de a păcăli nu numai clientul, dar și infrastructura tehnologică a instituției bancare, prin intermediul impersionării la nivel tehnic a clientului, prin intermediul unui API de comunicare/ interceptare/ menținere, astfel încât serverul băncii să mențină legătura cu ceea ce crede că este dispozitivul clientului, în timp ce atacatorul are acces deplin în contul clientului.

Referitor la folosirea API-ului pentru interceptarea / comunicarea/ menținerea autorizării accesului la sistemul bancar (2FA – 2 Factor Authentication / MFA – Multi Factor Authentication), așa cum am menționat anterior, conectarea clientului cu banca se face prin intermediul unei pagini false care interceptează și stochează datele de acces la contului bancar, iar după finalizarea activităților clientului pagina falsă continuă să păstreze activă legătura clientului cu serverul, chiar dacă acesta a părăsit platforma bancară.

Figura 4. Derulare atac phishing cu utilizare API de impresionare a clientului.
Sursă: Curs educație cibernetică – Atacul de tip phishing (https://www.cyberaid.eu/atacul-de-tip-phishing).

Clientul nu realizează în această etapă că a devenit victimă și nici tehnologia bancară nu poate depista acest lucru, deoarece clientul a validat accesarea contului prin user și parolă, plus autentificarea suplimentară prin SMS sau aplicație de autentificare (2FA/ MFA).

Complexitatea, impactul și implicarea ambilor factori decizionali (client și infrastructură bancară) în desfășurarea și reușita acestui atac cibernetic impune anumite schimbări în derularea comunicării dintre părți și se recomandă implementarea unor măsuri, ca cele de mai jos:

- Limitarea numărului de tranzacții
- Reducerea timpului de acces în sistem,
- Folosirea unei duble autentificări prin SMS (cu răspuns la SMS, nu cu completarea codului în platformă).
- Folosirea unei aplicatii de autentificare/confirmare instalata pe un terminalul mobil al clientului

Toate acestea acțiuni suplimentare sunt cronofage, dar pot preveni pierderi pentru clienți, cheltuieli pentru instituții, alterarea imaginii băncii etc..

2.4. Atac de tip pagină în pagină.

Conform descrierilor anterioare, un element important, dar problematic în același timp pentru atacatori, îl reprezintă adresa paginii false, care poate fi foarte asemănătoare cu cea a instituției bancare (banca_perferată.ro), poate conține părți componente din adresa oficială (banca_ta_preferată), cifre în locul literelor(banca_preferată.r0) sau poate fi o adresă a unei pagini web compromise la care se adaugă piese vizuale ”de convingere” (pagină_compromisă.ro/banca_preferată/ro/securizare/autentificare), dar care la o privire mai atentă poate crea suspiciuni utilizatorilor asupra autenticității paginii la care au ajuns.

Atacatorii au rezolvat această problemă, dezvoltatând o metodă de atac, prin intermediul căreia rata de succes este mai mare.

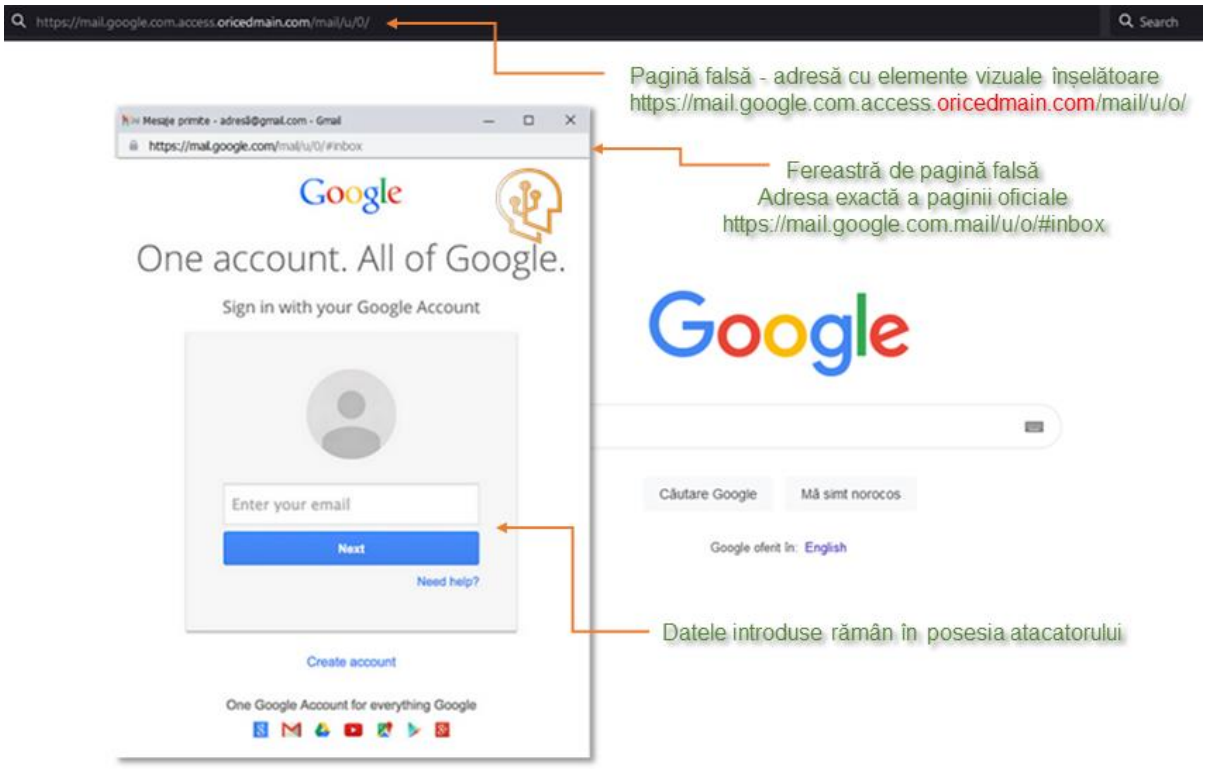

Figura 5. Exemplu de pagină falsă
Sursă: Prodefence cyber research team

Indiferent de adresa de la care pornește atacul, fie ea asemănătoare sau nu, la accesare paginii false utilizatorului i se va deschide o a doua fereastră falsă, care conține adresa oficială a instituției bancare, precum și toate elementele vizuale din zona de acces. Dacă adresa principală a paginii false ar putea alerta vizitatorul, cea de-a doua pagină afișează exact ceea ce conține pagina de acces oficială, oferind o mai mare credibilitate.

Odată introduse datele de acces, acestea vor intra în baza de date a atacatorului, iar victima va fi direcționată către infrastructura bancii.

Combaterea acestui tip de atac se face la fel ca în cazurile anterioare - prin blocarea exploatării resurselor și implicit identificarea sursei de la care se conectează clientul.

3. Educație – Informare – Avertizare

Prima linie de apărare din strategia generală de protejare a activelor și pasivelor se construiește prin educarea utilizatorilor finali. A doua linie de apărare o reprezintă soluțiile tehnice, care pot să prevină anumite atacuri în stadii incipiente, cum ar fi analiza nivelului de vulnerabilitate pentru a preîntâmpina materializarea amenințărilor, ceea ce conduce la o scădere a nivelului de expunere a factorului uman. A treia linie de apărare o reprezintă ajustarea cadrului legislativ și aplicarea de sancțiuni ca mecanism de descurajare.

Toate aceste abordări pot fi combinate pentru a crea soluții anti-phishing performante.

Unul dintre rolurile băncilor este de a-și ajuta clienții, de la primul contact al acestora cu tehnologia bancară, să înțeleagă realitatea și să perceapă gradul de pericol prin intermediul campaniilor de avertizare.

Trebuie combătut avantajul pe care îl au infractorii digitali asupra utilizatorilor cu o pregătire precară în domeniu. De asemenea, trebuie eliminate lacunele din politicile și procedurile bancare referitoare la contactarea clienților și la modalitatea de abordare a fenomenului infracțional, câteva dintre măsuri fiind propuse în cele de mai jos:

- să fie distribuite periodic (prin e-mail, sau direct pe site-ul web al băncii) informații generale despre phishing;
- să fie trimise clienților alerte despre înșelătoriile de tip phishing, mai ales atunci când este vizata direct o anumită bancă;
- să fie trimise memento-uri / remindere cu privire la politicile și procedurile privind contactarea clienților, astfel încât aceștia să fie capabili să recunoască solicitările neobișnuite. Banca trebuie să-și informeze de la început clienții în legătură cu aspectele generale și să explice foarte clar că „nu vă vom solicita niciodată parola sau informații confinețiale”, sau „modificarea datelor noastre de identificare bancare vor fi comunicate public, prin canale consacrate”, etc.

Atunci când băncile aleg să implementeze un program de conștientizare a clienților cu privire la phishing, este important să-și educe și angajații - în special angajații care interacționează cu clienții și care ar trebui să dețină informații solide despre acest subiect, astfel încât să poată răspunde la toată gama de întrebări .

Utilizatorii trebuie să fie educați / instruiți să raporteze către bancă și ulterior către instituțiile angajate în combaterea infracționalității orice tranzacție sau operațiune suspectă . Banca trebuie să explice în detaliu pașii care trebuie urmați în cazul în care un client suspectează că a devenit victimă și să-l sprijine în demersul său.

Banca trebuie să informeze clienții că raportările se fac în paralel sau concomitent cu cele către DNSC (Directoratul Național de Securitate Cibernetică) prin apelarea la numărul de telefon

1911, sau prin intermediul adreselor de e-mail de contact de pe site și către departamentele specializate ale Ministerului de Interne. Aceste aspecte sunt deosebit de importante deoarece mai multe raportări pot determina organismele abilitate să lanseze alerte de securitate cibernetică la nivel național și să preîntâmpine înregistrarea de noi victime. În funcție de gravitatea fenomenului se pot activa mecanisme care să antreneze și Departamentul Cyberint din cadrul Serviciului Român de Informații alături de alte instituții abilitate.

Avertizările constante prin mesaje de tip email și SMS le pot reaminti clienților faptul că banca nu solicită informații cu caracter confidențial și că nu trimite mesaje ”urgente” de blocare a conturilor. Trebuie depuse eforturi susținute pentru a schimba mentalitatea utilizatorului și pentru a susține dezvoltarea unei culturi orientate spre securitate cibernetică.

Sistemul bancar în relația cu clienții trebuie să schimbe radical strategia de abordare a subiectului, deoarece utilizatorii au tendința de a trata superficial anumite reguli, fie pentru că nu le cunosc, fie pentru că nu le înțeleg.

Concluzii

Deși educația cibernetică reprezintă una dintre cele mai eficiente bariere de apărare împotriva phishing-ului, această amenințare va fi dificil de eliminat complet datorită complexității în continuă creștere, a rafinamentului atacurilor, a elementelor de inginerie socială și a instrumentelor tehnice în continuă dezvoltare. Se poate observa o repoziționarea a agresorilor care trec de la e-mailurile tradiționale, la phishing-ul bazat pe rețelele sociale, înregistrându-se un permanent decalaj între atacurile de phishing sofisticate și contramăsurile implementate.

Campaniile de conștientizare cu privire la phishing trebuie să fie promovate nu doar clienților și angajaților băncilor, ci și personalului responsabil de aplicarea legii, care este în măsură să investigheze infracțiunile economico - financiare online. Clienții trebuie să cunoască nivelul potențialului impact financiar rezultat în urma unui atac cibernetic reușit. Băncile trebuie să încerce să combată capabilitățile în continuă schimbare ale atacatorilor cibernetici prin crearea de aplicații online adaptate, mai sigure, cu potențial de a recunoaște mai rapid schemele infracționale de tip phishing. Angajații care transferă fonduri în mod regulat, care gestionează date sensibile, sau care participă la activități cu risc operațional ridicat au nevoie de instruire suplimentară despre cum să detecteze și să evite capcanele phishing mai sofisticate. Persoanele cu rol de aplicare a legii trebuie de asemenea să fie familiarizate cu instrumentele utilizate în atacurile de tip phishing și să înțeleagă modul în care acestea funcționează, pentru a atribui corect atacurile făptuitorilor și pentru a propune contramăsuri mai eficiente.

Formarea continuă privind riscurile de securitate cibernetică poate fi cheia pentru a evita pierderile și pentru a reduce impactul. În acest articol s-a dorit evidențierea importanței dezvoltării mai multor tehnici anti-phishing, cu rol de detectare și blocare a atacurilor, precum și o taxonomie clară pentru a înțelege cât mai mult din ciclul de viață al phishing-ului.