RIINVEST
Departamenti i Shkencave Kompjuterike

Punim Diplome
Viti akademik 2020 - 2021

Engjëll Gashi

EVOLUCIONI I “PHISHING-UT”

Mentor: MSc. Blerim Jahiu

Shtator / 2021

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme
për Shkallën Bachelor

ABSTRAKT

Në kohën e tashme, sulmet kibernetike janë të paevitueshme për çdo entitet. Të gjitha entitetet si: Bizneset, korporatat, qeveritë apo edhe individualët bien pre e sulmeve kibernetike anembanë botës. Sulmet që ekzekutohen janë te natyrave te ndryshme por njëri ndër sulmet i cili ka qenë dhe është më se efektiv edhe ne ditët e sotme është sulmi “Phishing”. Një numër shumë i madh i këtij sulmi shpërndahet ne te gjithë boten, jo vetëm si një sulm gjeneral por edhe si një sulm i personalizuar ndaj një entiteti te veçante. Por gjëja më e çuditshme është se edhe pse “phishing”është metodë shumë e vjetër e sulmit, ende ka sukses në shumë raste. A është faji tek masat e sigurisë, rregulloret, edukimi, apo është thjesht gabim i njeriut. Në këtë temë do analizohet thellë se si ka evoluar “phishing”qe nga fillimet e tij dhe çfarë e bën atë një sulm kaq të përdorur nga hakerët edhe në ditët e sotme. Do analizojmë edhe ku janë pikat e dobëta që ta dimë se pse ky sulm ende ka sukses dhe do kuptojmë se çfarë mund të bëjmë që ta krijojmë një mjedis sigurie që është rezistent ndaj phishingut.

DEKLARATË E ORIGJINALITETIT

Unë, Engjëll Gashi deklaroj se: (1) Ky punim i diplomës përfaqëson punën time origjinale, përveç rasteve të citimeve dhe referencave dhe (2) Ky punim nuk është përdorur më parë si punim apo projekt në këtë kolegj apo në universitete/kolegje/institucione të tjera.

FALENDËRIME

Gjithmonë falënderues ndaj njerëzve të cilëve u takojnë meritat më të mëdha që unë sot përfundoj me sukses këtë kapitull. Falënderimi më i veçantë shkon për familjen time, të cilët më kanë dhënë përkrahjen më të madhe qe nga fillimi i rrugëtimit tim profesional duke më shtyrë që gjithmonë të arrija edhe ato qëllime që shumë herë mendova që do ishin te paarritshme me këshillat dhe afërsinë e tyre. Një falënderim special shkon edhe për të gjithë profesorët, ku secili me diturinë dhe aftësitë e tyre profesionale në aspektin teorik dhe praktik e bënë të mundur që leksionet e tyre të jenë sa më të kapshme për mua si student. Po ashtu një falënderim tjetër i veçantë shkon për mentorin Prof. Blerim Jahiu, ku përkrahja dhe përkushtimi i tij ka qenë një ndihmë shumë e madhe për mua që unë të arrij të përfundojë me sukses këtë kapitull. Gjithashtu, falënderoj shoqërinë dhe kolegët e mi të cilët e përcjellën rrugëtimin tim!

PËRMBAJTJA

LISTA E FIGURAVE

1. HYRJE

‘Phishing’ është një sulm i cili ka shumë kohë që është në përdorim. Nëse e përkthejmë direkt kjo fjale i bie ‘peshkim’, ku nënkuptohet se ky sulm përdoret për nxjerrjen e paautorizuar të të dhënave te një entiteti. Këto të dhëna mund të jene të natyrës së ndryshme. Të dhënat mund të jenë, username dhe password, numra te identitetit, numra të kartelës bankare apo ndonjë tjetër e dhëne sensitive. Ky sulm është një sulm i cili targeton përdoruesin dhe mund të jetë i personalizuar enkas për të. Përderisa përdoruesi mendon qe po i shtyp të dhënat tek faqja zyrtare e një kompanie apo po shtyp numrat e bankës tek banka e tij, ajo qe përdoruesi nuk e din është se edhe pse ne pamje duket tërësisht e njëjte, vendi ku ai po i shtyp te dhënat nuk është vendi zyrtar. Kjo rezulton ne ofrimin e te dhënave personale tek një person i paautorizuar i cili pasi ka qasje në to, e ka te mundur ti përdore ato qe te imitoje viktimën dhe të bëjë ç’të dojë me të dhënat e marra. Mund të duket shumë banale rënia pre e një sulmi të tillë pasi shumë njerëz mendojnë që është shumë e lehte të detektohet një sulm phishing, por e vërteta është që hakerët kanë arritur të bëjnë sulme “phishing” që i ngjasojnë faqes së vërtetë rreth 90%. Në pamje mund edhe të jetë komplet e njëjtë, por gjithmonë dallon tek domaini. Po ashtu e njëjta vlen edhe kur dërgohet email-i që përmban linkun e “phishing”. Email-i mund të duket komplet i njëjtë, por dallon se platformat me te famshme ne bote, asnjëherë nuk kërkojnë passwordin e përdoruesit. Nëse një email nga njëra nder këto platforma pranohet, atëherë është një shansë shume e madhe që ajo email të jetë një spam email e cila te ridrejton në një faqe “phishingu”. “phishing”nuk është gjithmonë i njëjtë, përkundrazi, ka shume lloje të këtij sulmi të cilat ne do i përmendim. Disa nga llojet siç janë: Email Phishing, SMS Phishing, Clone Phishing, Voice Phishing, CEO Fraud, Spear “phishing”. Në këtë hulumtim ne do shikojmë se si është zhvilluar sulmi i “phishing” ndër vite dhe do kuptojmë se cilat janë mënyrat me të mira që të evitohet një sulm i tille i suksesshëm. Do shikojmë llojet e phishingut, si ka evoluar ndër vite, do marrim edhe disa raste studimi te shikojmë se pse kane rezultuar të suksesshme ato sulme. Në fund të këtij hulumtimi ne do te arrijmë ne konkluzionet se çfarë mund të bëjmë që të ndihmojmë të gjitha entitetet që të parandalojnë apo detektojnë një sulm të tij në atë mënyrë që të mos bien pre e sulmit.

2. SHQYRTIMI I LITERATURËS

2.1.Historia e phishing-ut

"Phishing" ka filluar të përdoret që në kohët e hershme kur teknologjia ka filluar te evoluojë. Ky sulm ka kapluar të gjitha entitetet të cilat janë të lidhura në internet (Bizneset, Korporatat, Qeveritë, Individualet). Përdorimet e para janë regjistruar në kohën e viteve te 80-ta të cilat janë raportuar nga HP Users Group.[1] Hakeri Khan Smith ka filluar ta ambientoje këtë term gjatë viteve te 90-ta ku në një softuer për hacking (Hacking Tool) i cili quhej AOHell e ka përmendur "phishing"i cili ka bere të mundur që hakerët të merrnin në mënyrë të paautorizuar passwordet apo të dhënat bankare të përdoruesve të Portalit dhe ofruesit të shërbimeve America Online.[2] Pastaj vjen E-Gold ku pati po ashtu tentim te "phishing"i cili nuk ishte shume i suksesshëm.[3] Ne fundet e viteve 2003, hakerët filluan te blinin shume domains qe dukeshin si domain legjitim siç janë Paypal apo Ebay nëse nuk shikoheshin me vëmendje. Ata dërgonin emaila te shumta tek klientët e këtyre kompanive dhe klientët ofronin të dhënat e tyre personale duke menduar se po i ofrojnë ato të dhëna.[4]

Në fillimet e vitit 2004, hakerët po sulmonin shume me sukses faqet bankare dhe klientët e tyre. Pop-up dritaret u përdorën për të marrë informacion të ndjeshëm nga viktimat.[5] Midis majit 2004 dhe majit 2005, rreth 1.2 milion përdorues në SHBA pësojnë humbje të shkaktuara nga phishing, në total rreth 929 milion dollarë. Tash, organizatat humbasin rreth 2 miliardë dollarë në vit nga "phishing". [6]

Tashmë këto programe "phishing" po ashtu njihen si pjese e marketit te zi ku softuerët e reja kanë te implementuar edhe sistemet e pagesave. Kësaj dukurie i dha ndihme edhe lansimi i

[1] Felix, Jerry & Hauck, Chris (September 1987). "System Security: A Hacker's Perspective". *1987 Interex Proceedings*. **8**: 6. (qasur për herë të fundit më 25 Gusht 2021)
[2] "EarthLink wins $25 million lawsuit against junk e-mailer". Archived from the original on 2019-03-22. (qasur për herë të fundit më 25 Gusht 2021)
[3] "GP4.3 – Growth and Fraud — Case #3 – Phishing". *Financial Cryptography*. December 30, 2005. (qasur për herë të fundit më 26 Gusht 2021).
[4] "phishing". org Editor, (qasur për herë të fundit më 25 Gusht 2021) , tek https://www."phishing". org/history-of-phishing (qasur për herë të fundit më 25 Gusht 2021)
[5] Po aty.
[6] Po aty.

bitcoin në vitin 2008, ku lejoi që transaksionet të bëhen në mënyrë të sigurt dhe anonime, duke ndihmuar hakerët të fshiheshin edhe më mirë.

2.2.Si funksionon phishing

Zakonisht përdoret për të marrë të dhëna të ndieshme të ndonjë entiteti. Varësisht nga lloji i phishing-ut që përdoret, në shumicën e rasteve procesi shkon si me poshtë:

1. Hakeri merr një domain i cili duket përafërsisht i njëjtë me target domainin
2. Ai e dizajnon qe te duket tërësisht i njëjte si target domaini.
3. Zgjedhet një viktimë potenciale dhe i dërgohet një email ku në të cilën detyron viktimën që të klikojë ne një link i cili e ridrejton viktimën tek "phishing" domaini.
4. Viktima duke mos e analizuar domainin mire, plotëson fushat dhe te gjitha te dhënat shkojnë tek hakeri.

Pos kësaj, ekziston edhe "phishing" mobil, i cili zakonisht dërgohet direkt ne telefonin e një përdoruesi. Procesi për "phishing" mobil vazhdon si më poshtë:

1. Hakeri merr një numër të madh të numrave te telefonit apo vetëm numrin e viktimës potencial.
2. Dizajnon një mesazh i cili i kërkon viktimës të përditësojë të dhënat, të ndërroje një password apo ndonjë mesazh të këtij lloji.
3. Viktima klikon ne linkun e ofruar duke rezultuar në një vizite në një ueb faqe false.
4. Viktima i ofron te dhënat e ndjeshme (rëndësishme) të hakerit.

Duhet te përmendet se sulmet e "phishing" mobil kane shume me shume gjasa te ekzekutohen me sukses për shkak se ne telefon nuk dihet gjithmonë se kush është dërguesi i mesazhit dhe po ashtu ne telefon nuk shihet domaini i plote.

Më poshtë do shohim disa raste të një sulmi "phishing" dhe si mund ta dallojmë se a është një sulm apo një email legjitim.

2.3. Llojet e phishing

"Phishing" ka shume lloje dhe mënyra te ndryshme në bazë të te cilave mund te ekzekutohet. Pasi detyra e këtij sulmi është të mashtrojë viktimën që të ofrojë të dhënat e tij personale, atëherë hakerët e kanë parë të arsyeshme të zhvillojnë metoda të reja që të mashtrojnë përdoruesit që të ofrojnë kredencialet e tyre. Edhe pse sulmet filluan me phishing mesazhe të thjeshta, hakerët arritën të zhvillojnë teknika dhe metoda të ndryshme sulmi phishing, jo vetëm me mesazhe gjenerale, por edhe mesazhe të personalizuara apo edhe mesazhe me zë ku imitohej një person në pozitë të lartë në kompaninë ku përdoruesi gjendej. Disa nga llojet kryesore të "phishing" sulmit janë këto që përmenden më poshtë.

2.3.1. Email Phishing

Email "phishing" është metoda me e famshme dhe e zakonshme e "phishing". Me email "phishing" përdoruesit i dërgohet një email, në atë email mund të ceket se është e detyrueshme që të përditësohet passwordi i platformës. Në momentin që përdoruesi klikon atëherë linku e dërgon atë në një uebfaqe klon e cila nuk është legjitime ku përdoruesi i jep hakerit të dhënat personale duke dhënë inputin në ueb faqen klon.[7]

2.3.2. Spear Phishing

Është një metodë me efektive dhe me speciale e "phishing". Kjo metode bën që hakeri të krijoje një "phishing"te personalizuar për targetin e tij pasi që ka marre te dhëna personale për targetin duke ditur te dhënat publike te targetit. P.sh. nëse hakeri e di qe targeti i tij ka një llogari në një platforme si Netflix, atëherë hakeri i dërgon atij një email të personalizuar që të ndërrojë passwordin e llogarisë se tij.[8] Kjo e-mail e dërgon viktimën tek një website klon ku viktima i ofron të dhënat e tij hakerit. Në këtë mënyrë rezulton phishingu i suksesshëm nga ana e hakerit.

[7] Kasey Hewitt, Maj 2021, *12 Types of "phishing"Attacks and How to Identify Them, tek* https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them (qasur për herë të fundit më 26 Gusht 2021)
[8] Po aty.

2.3.3. CEO Fraud

Hakeri përdorë një email te njohur për viktimën, p.sh., një email te ngjashëm me emailin e punëdhënësit apo drejtorit ekzekutiv. Në këtë sulm hakeri i kërkon përdoruesit që të kryejë një transaksion apo t'i japë atij të dhëna të ndjeshme për kompaninë. Po ashtu i bën me dije se nuk ka shumë kohë. Viktima në këtë rast gjendet në presion dhe në kohë të shkurtë, duke e shtyrë atë që ti plotësojë kërkesat e hakerit.[9]

2.3.4. Content Injection

Hakeri merr qasje të paautorizuar në një uebfaqe apo platformë. Në atë platformë viktima ka një llogari për të cilën hakeri e di. Atëherë ai krijon një faqe ekstra brenda platformës dhe i kërkon viktimës që të kyçet në të apo edhe të shkarkojë ndonjë file nga serveri. Kjo rezulton në humbjen e kredencialeve të përdoruesit apo instalimin e një virusi tek përdoruesi.[10]

2.3.5. Session Hijacking

Hakeri merr qasje ne ueb serverët e kompanisë dhe marrin direkt fajllat nga serveri ne mënyrë te paautorizuar.[11]

2.3.6. Mobile "phishing"(Smishing)

Hakeri i dërgon mesazh ne telefon viktimës duke i kërkuar që të klikojë linkun që të shkojë në ueb faqe dhe të ndërroje apo përditësojë te dhënat. Nëse viktima klikon, mund të instalojë malware në telefonin e tij apo te ridrejtohet ne një ueb faqe e cila ka për qëllim ti marrë të dhënat e viktimës.[12] Duhet të ceket se "Smishing" është një ndër teknikat që është shumë e vështirë të dallohet pasi që kur klikohet linku i dërguar në mesazh nuk shihet i tërë domain-i por vetëm një pjesë.

[9] Po aty.
[10] Po aty.
[11] Po aty.
[12] Po aty.

2.3.7. Voice “phishing”(Vishing)

Hakeri i lë një mesazh me zë viktimës duke i thënë ta thirrin në një numër tjetër. Në numrin tjetër hakeri bisedon me viktimën duke imituar një person legjitim si një drejtor ekzekutiv apo ndonjë administrator banke, duke e detyruar viktimën të ua kryejë shërbimet.[13] Në vitet e fundit hakerët kanë arritur qe të përdorin po ashtu ndryshues të zërit që ta ndryshojnë zërin dhe duke e bërë identik si zëri i personit që ata duan ta imitojnë.

2.3.8. Man-In-The-Middle

Ne këtë metodë hakeri iu dërgon “phishing” email dy personave. Të dy personat mendojnë se janë duke biseduar me njëri tjetrin dhe komunikimi është i sigurt, kurse ne fakt, email-at e te dyve shkojnë tek hakeri dhe ai i manipulon të dy te shpërndajnë te dhëna konfidenciale.[14] Ai e sheh të gjithë trafikun që qarkullon dhe arrin të ndërrojë mesazhet dhe të dërgojë mesazhin e dëshiruar në mënyrë që të mashtrojë të dy palët.

2.3.9. Malvertising

Malvertising i përdor në shumicën e rasteve dritaret “pop-up” apo reklamat e klikueshme në ueb faqe të ndryshme. Nëse përdoruesi klikon në to, mund të instalojë një virus në pajisjen e tij. Po ashtu përdoren shumë edhe browser “pop-ups” ku i kërkohet përdoruesit që ta lejojë apo ta refuzojë një qasje të caktuar.[15]

[13] Po aty.
[14] Po aty.
[15] Po aty

2.4.Statistika për phishing gjatë viteve

Siç e kuptuam deri tani, "phishing" ka një kohë të gjatë që gjendet në mjedisin kibernetik dhe është një sulm i cili çdo vit shkon duke u shumëfishuar dhe duke u bërë më efektiv se që ishte një vit më parë.

Më poshtë kemi një listë me fakte dhe statistika për "phishing" të cilat do na japin një kuptim më të mirë sa i përket këtij lloji të sulmit.

Lista e mëposhtme është mbledhur nga 'phishingbox'.[16]

- 33% e sulmeve "phishing" janë sulme sociale.[17]
- 65% e grupeve sulmuese kanë përdorur spear "phishing" si vektor primar të infektimit.[18]
- 29% e thyerjeve kanë përfshirë kredenciale të vjedhura.[19]
- 48% e emaileve me qëllim të keq kanë pasur të bashkangjitur fajlla të Office.[20]
- 94% e viruseve janë dërguar me email.[21]
- 32% e thyerjeve kanë përfshirë "phishing".[22]
- 64% kanë hasur në "phishing" në vitin 2017.[23]
- 22% e organizatave e shohin "phishing" si njëri ndër kërcënimet më të mëdha të sigurisë së asaj kompanie.[24]
- 59% e sulmeve te "phishing-ut" janë të lidhura me financat sa i përket Shteteve Të Bashkuara.[25]
- 85% e organizatave kanë treguar se raportimet e sigurisë nuk janë në nivel të duhur dhe nuk i arrinin pritshmërinë e tyre.[26]

[16] Phishingbox Editor, "phishing"Facts, tek https://www.phishingbox.com/resources/phishing-facts
[17] Verizon Data Breach Investigations Report (DBIR) 2019 (qasur për herë të fundit më 9 Shtator 2021)
[18] Symantec Internet Security Threat Report (ISTR) 2019 (qasur për herë të fundit më 9 Shtator 2021)
[19] Verizon Data Breach Investigations Report (DBIR) 2019 (qasur për herë të fundit më 9 Shtator 2021)
[20] Symantec Internet Security Threat Report (ISTR) 2019 (qasur për herë të fundit më 9 Shtator 2021)
[21] Verizon Data Breach Investigations Report (DBIR) 2019 (qasur për herë të fundit më 9 Shtator 2021)
[22] Po aty
[23] Check Point Research Security Report 2018 (qasur për herë të fundit më 9 Shtator 2021)
[24] EY Global Information Security Survey 2018 (qasur për herë të fundit më 9 Shtator 2021)
[25] NTT Security Global Threat Intelligence Report 2018 (qasur për herë të fundit më 9 Shtator 2021)
[26] EY Global Information Security Survey 2018 (qasur për herë të fundit më 9 Shtator 2021)

- 70% e thyerjeve që kanë qenë të shoqëruara me akterë të shteteve apo kombeve të ndryshme kanë qenë të lidhur me sulmin “phishing”. [27]
- 74% e sulmeve të spiunazhit kibernetik kanë përfshirë metodën e “phishing”. [28]
- 90% e incidenteve apo thyerjeve kanë përfshirë së paku një element të “phishing”.[29]
- Nga 2015 në 2016, është rritur hapja e mesazheve të llojit “phishing”nga 23% në 2015 në 30% në 2016.[30]
- 70% e sulmeve kibernetike përdorin një kombinim të metodave të ndryshme të “hacking” por gjithmonë duke e përdorur edhe ndonjë vektor të “phishing”. [31]
- Norma e një “phishing”email-i është 1 në 1,846.[32]
- Anti Phishing Working Group (Grupi Punues kundër “phishing”) apo APWG në vitin 2016 ka deklaruar se çereku i parë i vitit 2016 ka pasur më shumë sulme se çdo vit tjetër që nga viti 2004.[33]

2.5.Phishing gjatë pandemisë

Viti 2020 ka qenë një vit shumë më ndryshe, shkaku i një pandemie e cila shtyu shumicën e bizneseve të ktheheshin në biznes digjital, e cila nënkuptonte një fazë të re zhvillimi por po ashtu një shumëzim të sulmeve kibernetike. Në vitin 2020, 75% e organizatave rreth botës kanë hasur në sulme të phishingut, dhe është shqetësuese fakti se 74% e sulmeve që kanë pasur në shënjestër bizneset amerikane dhe i kanë sulmuar ato, kanë rezultuar si sulme të suksesshme.[34] Ka shumë biznese të cilat thonë se u ofrojnë stafit të tyre trajnime të ndryshme sa i përket vetëdijesimit të sigurisë kibernetike, prapë “phishing” është njëri ndër kërcënimet që ka potencial shumë të madh që të thyejë mbrojtjet e kompanive. Siç është përmendur më herët, sipas raportit të Verizon të vitit 2020, 22% nga të gjitha thyerjet janë sulme të cilat e përdorin “phishing”. Edhe Qendra e

[27] Verizon Data Breach Investigations Report (DBIR) 2018 (qasur për herë të fundit më 9 Shtator 2021)
[28] Po aty
[29] Verizon Data Breach Investigations Report (DBIR) 2017 (qasur për herë të fundit më 9 Shtator 2021)
[30] Verizon Data Breach Investigations Report (DBIR) 2016 (qasur për herë të fundit më 9 Shtator 2021)
[31] Po aty
[32] Symantec Internet Security Threat Report 2016 (qasur për herë të fundit më 9 Shtator 2021)
[33] Anti-”phishing”Working Group (APWG) (qasur për herë të fundit më 9 Shtator 2021)
[34] Caitlin Jones, 50 “phishing”Stats You Should Know In 2021, https://expertinsights.com/insights/50-phishing-stats-you-should-knoë/#The%20Frequency%20Of%20Phishing%20Attacks (qasur për herë të fundit më 9 Shtator 2021)

Ankesave te Krimeve të Internetit (IC3) e cila është qendër nga FBI, ka pranuar një numër të madh të ankesave gjatë vitit 2020. Ata kanë treguar se phishing, vishing, Smishing dhe pharming, kanë qenë disa nga sulmet më të shumta gjatë vitit 2020, dhe kanë lënë pas 241,342 viktima.[35] Këto sulme kanë përfshirë jo-pagesë / jo-dërgim (108,869 viktima), shantazh(76,741 viktima), thyerje të të dhënave personale (45,330 viktima) dhe vjedhje e identitetit (43,330 viktima).[36]

Ne lirisht mund të themi se pandemia e COVID-19 edhe ka ndikuar që të hapen sytë më shumë ndaj sigurisë kibernetike në të gjithë botën. Nje ndër kompanitë që merret me auditime, konsultime, këshilla financiare apo risku etj., Deloitte, ka zbuluar se pandemia ka ndikuar tek siguria kibernetike duke rritur rrezikun, rritur numrin e kriminelëve kibernetik, gjetje e dobësive të reja fizike dhe ato të sigurisë të informacionit.[37]

Në pandemi ka pasur 300% rritje të krimeve kibernetike të cilat janë raportuar, e kjo statistikë është vetëm në Shtetet e Bashkuara të Amerikës[38]. Kurse kemi po ashtu kompani të mëdha si Google, që ka raportuar se në baza ditore, Google ka mundur të shohë rreth 18 Milionë email-a që kanë përmbajtur Viruse apo "phishing" email-a që kanë pasur si tematikë kryesore një lidhje të caktuar me COVID-19, kurse mesazhet spam kanë qenë në numër edhe më të madh, duke arritur shifrën 240 Milionë.[39]

Duke marrë parasysh se popullata e botës është rreth 7.9 Miliardë, mund të themi se një përqindje e vogël është e inkuadruar në krime kibernetike, por, përkundrazi, ajo përqindje e vogël është shumë e madhe për shkak se dëmet e krimeve kibernetike në vit kalojnë disa trilionë dollarë.

[35] Po aty.
[36] Po aty.
[37] Packetlabs Editor, Cybersecurity Statistics about COVID-19, 2021, tek https://www.packetlabs.net/cybersecurity-statistics-2021/ (qasur për herë të fundit më 9 Shtator 2021)
[38] Po aty.
[39] Po aty.

2.6.Phishing në kohën aktuale

Nuk është e vështirë të kuptohet se nuk jemi duke i përballuar siç duhet sulmet kibernetike që ndodhin çdo ditë. Pritet që vetëm krimi kibernetik ti bëjë dëme botës diku rreth 6 Trilionë Dollarë kurse në 2025 pritet që numri të rritet deri në 10.5 Trilionë Dollarë.[40]

Rreth 61% të profesionistëve të sigurisë kibernetike besojnë që ekipi e tyre nuk ka staf mjaftueshëm, dhe në këtë vit, janë rreth 3.5 Milionë vende të lira pune vetëm sa i përket kësaj dege. [41] Mund të themi se "phishingu" rri rreth vendeve të para në listë si njëri ndër sulmet kibernetike më të përdorura, për shkak se vetëm nga viti 2020, ku 22% e thyerjeve kanë përfshirë phishing, kjo statistike në këtë vit (2021), është rritur ne 36%. Duhet po ashtu të llogarisim se në vitet 2019 dhe 2020, shkalla e suksesit të një sulmi "phishing" drejtuar organizatave është rritur nga 55% deri më 57%.[42]

2.7.Si ka evoluar Phishing?

Phishing ne fillim ka qenë shumë i thjeshtë ku edhe dizajni i phishingut ka qenë jo-profesional. Pasi që hakeret filluan të bënin dizajne, ata vazhduan duke bërë fushata të mëdha "phishing" ku të njëjtin "phishing" e dërgonin tek mijëra emaila. Edhe pse ka akoma fushata masive që synojnë këdo që do të klikojë një link, sulmet e tjera të "phishing" janë shumë më të mira dhe më të sakta.[43] Spear Phishing, për shembull, synon individë ose organizata të veçanta që përdorin ueb faqe me të cilat ata janë të familjarizuar ose imitojnë individë të njohur për ta në mënyrë që t'i joshin ata.[44] Whaling është edhe më e saktë, drejtuar ndaj ekzekutivëve të kompanive. Nga atje, një email është krijuar për të personalizuar përmbajtjen dhe për të përcjellë tonin e duhur për biznesin ose individin. [45]

Kohëve të fundit, ka shumë më shumë njerëz që kanë aftësi për të bërë "phishing". Më parë, aktorët kërcënues ishin vetëm ata që kanë kuptuar mekanikën e "phishing". Tani, "phishing"

[40] Po aty.
[41] Po aty.
[42] Po aty.
[43] CoreSecurity Editor, (Nxjerrur me Gusht 2021), *How "phishing"Has Evolved and Three Ways to Prevent Attacks* tek *https://www.coresecurity.com/blog/how-phishing-has-evolved-and-three-ways-prevent-attacks*
[44] CoreSecurity Editor, (Nxjerrur me Gusht 2021), *How "phishing"Has Evolved and Three Ways to Prevent Attacks* tek *https://www.coresecurity.com/blog/how-phishing-has-evolved-and-three-ways-prevent-attacks*
[45] Po Aty.

programet mund të blihen lehtësisht në dark ueb apo në ueb faqen e errët, duke i dhënë pothuajse kujtdo që ka dëshirën të bëjë këtë sulm mjetet e nevojshme për ta bërë këtë.[46] Kjo ka ndihmuar në rritjen e sasisë së sulmeve dhe efektivitetin e tyre.

Njëri ndër evoluimet e mëdha ka qenë edhe mundësia që të instalojnë certifikata false të enkriptimit në ueb faqet e phishingut, duke i dhënë viktimës një ndjenjë false sigurie dhe duke 'verifikuar' se ueb faqja klon është ueb faqe legjitime. Sipas mendimit tim, evolucioni më i madh ka qenë kur me anë të inteligjencës artificiale, hakerët kanë përdorur një softuer i cili ka mundësuar ndryshimin e zërit duke imituar personin ekzekutiv të kompanisë. Mund të themi se hakerët janë gjithmonë disa hapa para inxhinierëve të sigurisë kibernetike duke krijuar metoda të reja të sulmit dhe kjo paraqet një sfidë të madhe për ekipen mbrojtëse, dukë i shtyrë që të jenë më të shpejtë dhe më kreativ në krijimin e teknikave të reja mbrojtëse.

[46] Po Aty.

3. DEFINIMI I PROBLEMIT

Në çdo hulumtim i cili bëhet, është e domosdoshme te dihet arsyeja për temën për të cilën po behet hulumtimi, çfarë sfide ne shoqëri paraqet, pse është ende ekzistuese ne shoqëri kjo dukuri dhe cilat mund te jene zgjidhjet adekuate për te. E gjitha kjo mund te arrihet me shtrimin e pyetjeve hulumtuese apo kërkimore të cilat na mundësojnë te hyjmë shumë më thellë në temën e caktuar dhe të mos e shohim problemin vetëm sipërfaqësisht. Këto pyetje gjithmonë e më shume do na afrojnë tek zgjidhjet më të mira që të ulet kjo dukuri ose nëse është e mundur edhe të zhduket tërësisht. Në rastin tone, evolucioni i “phishing” na lejon të bëjmë pyetje si:

1. Si ka evoluar “phishing” ndër kohë?
2. Pse ky sulm është ende efektiv?
3. A ekziston mbrojtje ndaj këtij sulmi?
4. Si mund të ulim ratën e suksesit dhe të rrisim vetëdijesimin e njerëzve ndaj këtij sulmi?

4. METODOLOGJIA

Në këtë punim do të përdoren të dhëna sekondare. Do përdoret metoda kualitative për nxjerrjen e të dhënave që do na ndihmojnë të mbërrijmë në një konkluzion sa më të saktë. Po ashtu do perdoret metoda analitike qe te dimë ndikimin e evolucionit të phishingut në jetën e njerëzve. Do përdoret edhe metoda krahasuese, ku do krahasohet suksesi i sulmit në kohën e kaluar dhe tash, dhe po ashtu do të krahasohet se sa janë te vetëdijshëm njerëzit tani kundrejt kohës se kaluar. Do analizojmë të dhëna nga raporte, artikuj dhe hulumtime tjera qe janë relevante për temën të cilën po e trajtojmë. Do përdoren edhe burime kredibile dhe të sigurta nga interneti siq janë raportet vjetore nga Anti Phishing Working Group, Symantec Security, Raportet vjetore të sigurisë nga Verizon etj.

5. RASTE STUDIMI

5.1.Rast Studimi As Online

Deri më tani kuptuam se sulmet “phishing” janë ende shumë të suksesshme. Personalisht edhe unë kam pasur rastin të përballem me sulme të llojit të tillë. Një ndër kompanitë që më ka kontaktuar sa i përket këtij problemi ka qenë edhe kompania kreative digjitale “as online” e cila gjatë vitit 2018 në platformën e saj në instagram ka pasur mbi 500,000 ndjekës. Mënyra se si kjo kompani u sulmua ka qenë shumë më specifike dhe më poshtë do prezantojmë se si kjo kompani ra pre e phishing-ut, duke humbur të gjitha rrjetet sociale dhe po ashtu të ofrojmë mundësi se si ky sulm ka mundur të evitohej. Sulmi edhe kësaj here ka ndodhur përmes një email-i, ku u kontaktua një punonjës i kompanisë i cili ka pasur pozitën e publikuesit të imazheve/videove në rrjetin social të instagramit. Punonjësin do ta quajmë Tom (jo sipas emrit të vërtetë). E-maili si temë kryesore ka pasur verifikimin e llogarisë së kompanisë në instagram. Verifikimi në instagram është proces i cili i ofron një shenjë validimit llogarisë duke e bërë të ditur se ajo llogari është llogari origjinale. Vlen të përmendet, se, kompania ka dërguar kërkesë në instagram për verifikimin e llogarisë rreth një muaji më parë, fakt ky që ka ndikuar që Tomi të mos dyshonte fillimisht që ky e-mail të ishtë email i “phishing” dhe duke i dhënë atij një ndjenjë euforie, gjë që ka ndikuar që ai të mos i shikojë detajet. Pasi Tomi vetëm u ka ofruar besimin hakerëve, atëherë ai klikon në një buton i cili e bën redirekt tek një faqe klon e instagramit e cila i kërkon një username dhe një password. Pa hezituar ai i plotëson të dyja. Pas kësaj, hakerët vazhdojnë duke i dërguar një email tjetër ku nga Tomi kërkohet të bëjë një foto duke mbajtur në dorë kodin e sigurisë që i’u dërgua. Tomi i dërgon edhe fotografinë, duke i dhënë qasje sulmuesit në e-mail dhe instagram fillimisht, i cili ndërroi të gjitha të dhënat për të ndaluar qasjen e Tomit, dhe kjo rezultoi në dhënien e qasjes edhe të rrjeteve të tjera sociale. Pra, nga një lëshim i vogël, sulmuesi arriti të marrë qasje në të gjitha rrjetet sociale. Fatmirësisht, këto të gjitha u kthyen për shkak se kompania kishte të dhënat fillestare me të cilat janë hapur llogaritë. Pyetja shtrohet se si do mund të evitohej ky rast?

Së pari, përmendim gabimin e parë, i cili ka qenë gabimi se fjalëkalimet kanë qenë të njëjta për të gjitha rrjetet sociale. Përndryshe, ky sulm nuk do kishte sukses nëse vetëdijesimi i sigurisë kibernetike do ishte më i madh, apo nëse Tomi apo ndonjë punonjës tjetër i kompanisë do kishte

vetëdijesim të sigurisë kibernetike. Dhe kjo mungesë e vetëdijesimit së bashku me phishingun i cili ka qenë i punuar mirë dhe në mënyrë profesionale, ka bërë të mundur që ky sulm të jetë i suksesshëm.

5.2.Rast Studimi Shopify

Sa i përket këtij rasti, kompania në të cilën kam punuar nuk më ka lejuar që të publikoj të dhënat e tyre apo të përdor të dhënat e marra gjatë hulumtimit, por më ka dhënë mundësinë që të përdori dijeninë që kam fituar gjatë atij hulumtimi. Gjatë punës në këtë kompani kanë ardhur emails direkt në inbox dhe këto email kanë qenë të natyrës “phishing”. Pasi unë klikoja në buton, butoni më dërgonte në një faqe klon. Më e çuditshmja ka qenë se edhe kur e shikoja se kush e kishte dërguar email-in, burimi ka qenë nga e-maili legjitim. Pra, isha duke u përballur me një haker i cili kishte qasje në e-mail legjitim të një kompanie të njohur ndërkombëtarisht. Menjëherë, vazhdova të hulumtoja mailer-ë të ndryshëm por asënjëri nga ta nuk sillte rezultatet e duhura. Ishin të shtrenjtë, nuk mund të përdorje email domains të ndryshëm por vetëm email domains të blerë. Pyetja që kisha në kokë ishte se si mundej dikush të dërgonte një email e cila është phishing, emaili vinte nga një domain email legjitime dhe po ashtu nuk shkonte në spam por vinte direkt tek mesazhet. Provova të rikrijoja sulmin por gjithmonë pa sukses, pa domain email dhe po ashtu sulmi shkonte direkt në spam. Pas disa kohësh që mendoja ‘jashtë kutisë’ kuptova se ishte çështje e dobësisë së logjikës së biznesit. Dhe duke përdorur një platformë ekzistuese, arrita të rikrijoj sulmin dhe zbulova që shumë gjëra të vogla më kanë ikur. Më poshtë do sqarojmë se si ka qenë rrugëtimi ynë për zbulimin e këtij sulmi.

Hapi 1. Krijo një llogari në shopify. Këtu krijojmë një llogari të rrejshme vetëm për testim.

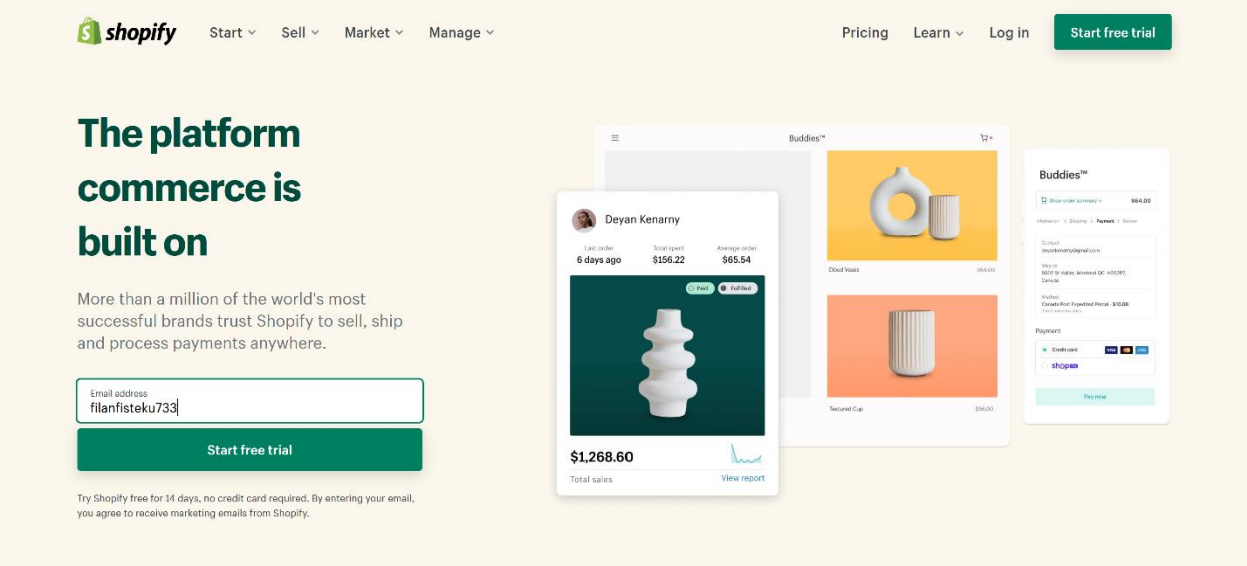


Figura 1. Shopify Faqja Kryesore.

(Burimi: www.shopify.com)

Hapi 2. Ofro të dhënat të cilat mund po ashtu të jenë jo të vërteta.

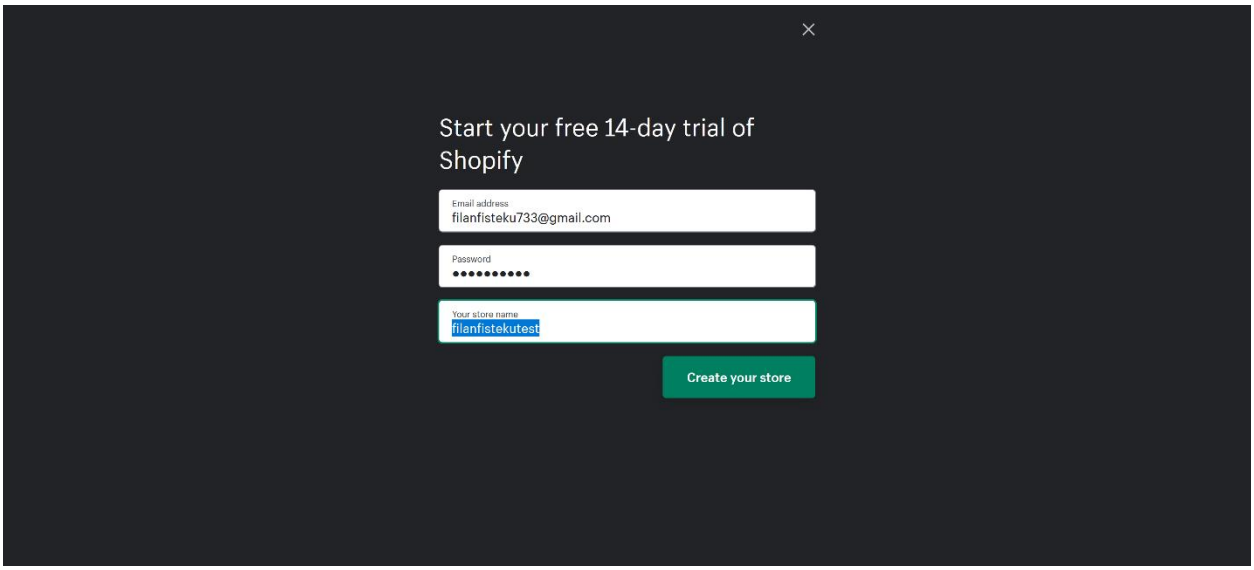


Figura 2.Krijimi i llogarisë Shopify.

(Burimi: www.shopify.com)

Hapi 3. Regjistro një klient. Ky hap është hap shumë me rëndësi dhe bëhet për shkak se platforma shopify e ka opsionin “Customer agreed to recieve marketing emails”. Kjo na bën të

kuptojmë se ne mund të regjistrojmë manualisht persona në dyqanin tonë dhe t'u dërgojmë emails të ndryshme që nuk shkojnë në spam.

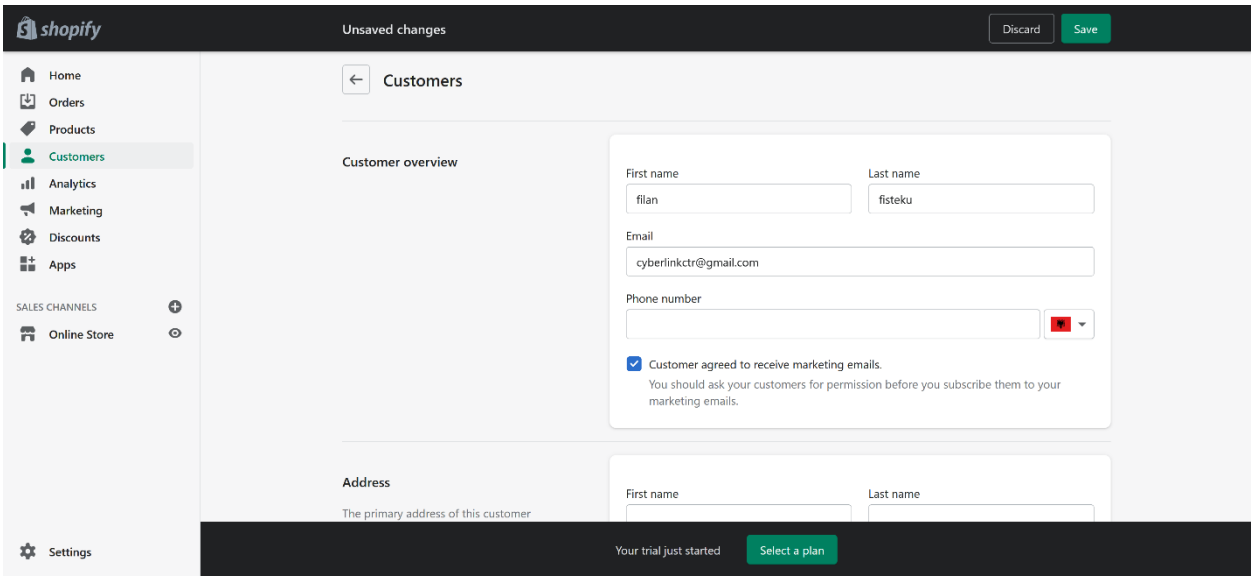


Figura 3. Regjistrimi i klientit.

(Burimi https://filanfistekutest.myshopify.com/admin/customers)

Hapi 4. Ndërrojmë emrin e dyqanit dhe emailin e dërguesit. Këtu kuptojmë se si hakeri ka qenë në gjendje të përdorë email domains të ndryshëm dhe ta bëjë sulmin të dukej kaq legjitim. Këtu mund të shihet se kam ndërruar edhe emrin e dyqanit por edhe emailin e dërguesit.

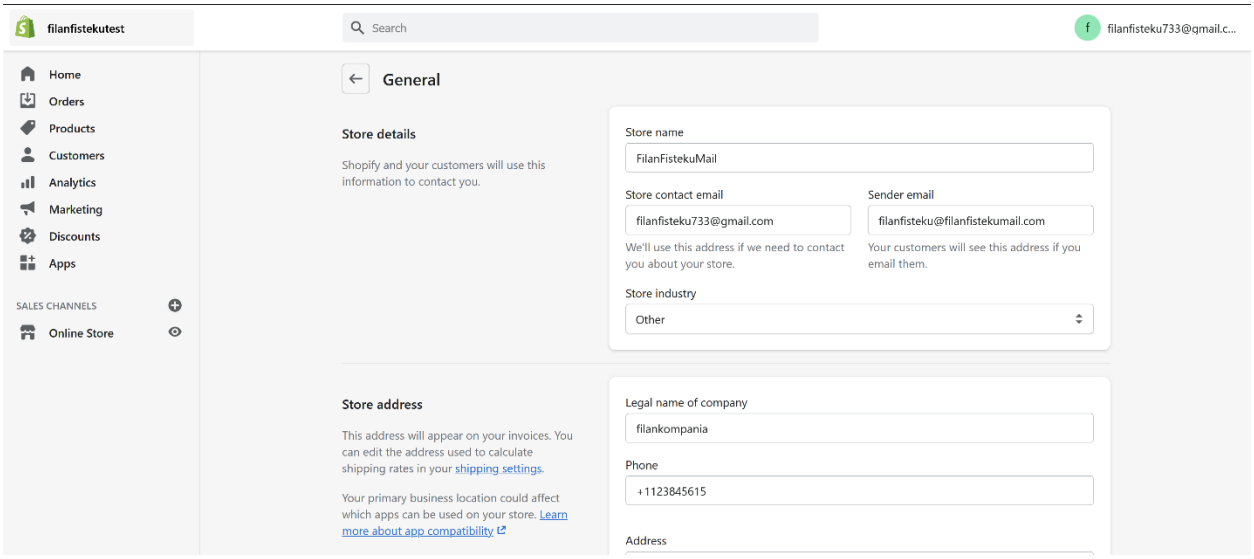


Figura 4. Ndërrimi i emailit të dërguesit dhe emrit të dyqanit.

(Burimi: https://filanfistekutest.myshopify.com/admin/settings)

Hapi 5. Shkojmë tek menyja e shopify dhe klikojmë tek marketing > Shopify Email.

Kjo na mundëson që të përdorim një vegël e cila do u dërgojë emaila promocioni tek klientët e dyqanit, e cila na tregon ne se një haker mund ta përdorë këtë të dërgojë kampanja “phishing”tek shumë njerëz.

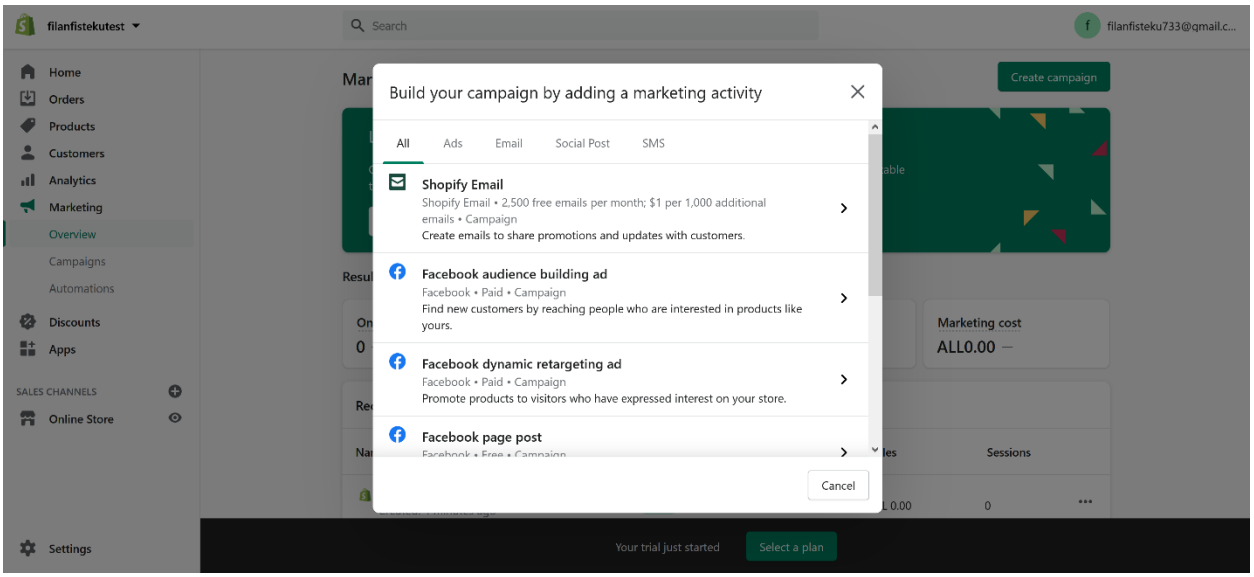


Figura 5. Krijimi i kampanjës së emailave.

(Burimi: filanfistekutest.myshopify.com/admin/marketing)

Hapi 6. Krijojmë një email dhe provojmë Send Test. Problemi që shfaqet është se platforma nuk na lejon të dërgojmë emails pa e paguar. Por nuk do të thotë që nuk ka mënyra tjera për ta kapërcyer këtë pengesë.

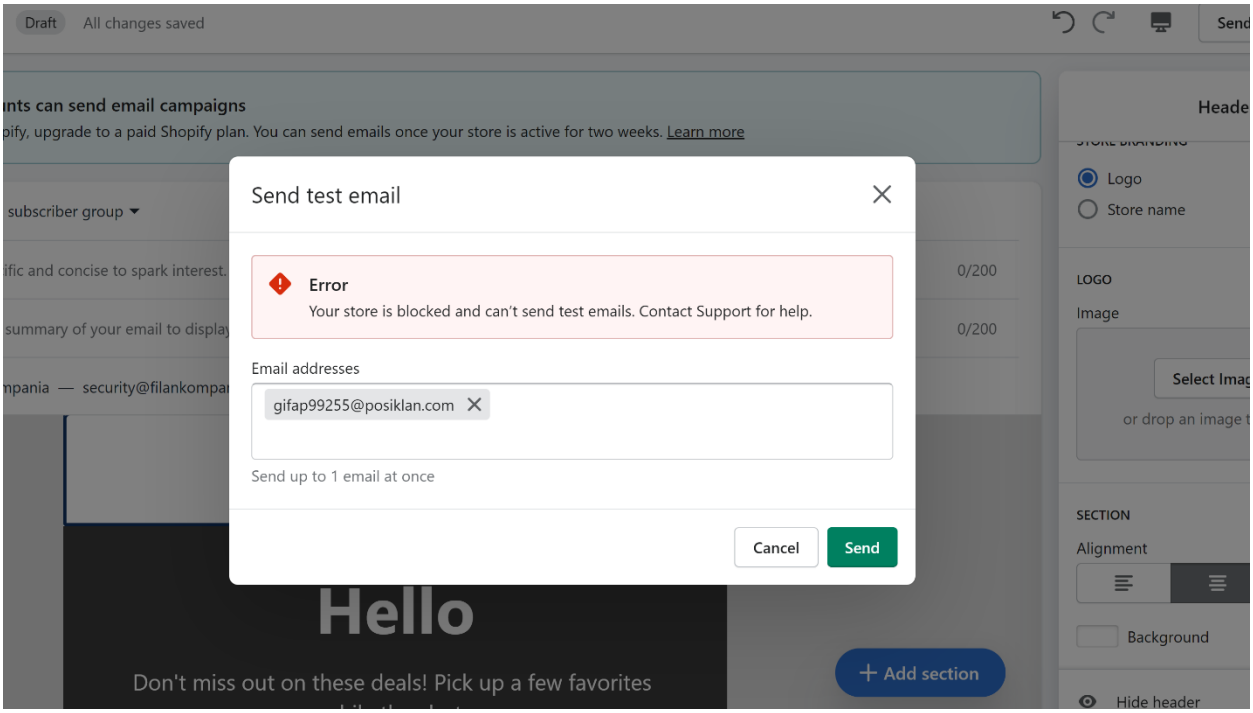


Figura 6. Nuk na lejohet të dërgojmë email.

(Burimi: https://filanfistekutest.myshopify.com/admin/apps/shopify-email/editor/3662664)

Hapi 7. Shkojmë tek Settings > Notifications dhe tek New Orders. Aty shtojmë një email tek 'Add Recipient' dhe dizajnojmë emailin tamam siç duam ne. Po ashtu kemi edhe opsionin që të ngarkojmë kod HTML duke e bërë emailin edhe më të besueshëm. Pasi klikojmë në Send Test Notification atëherë dërgohet direkt një email tek emaili i cili po sulmohet.

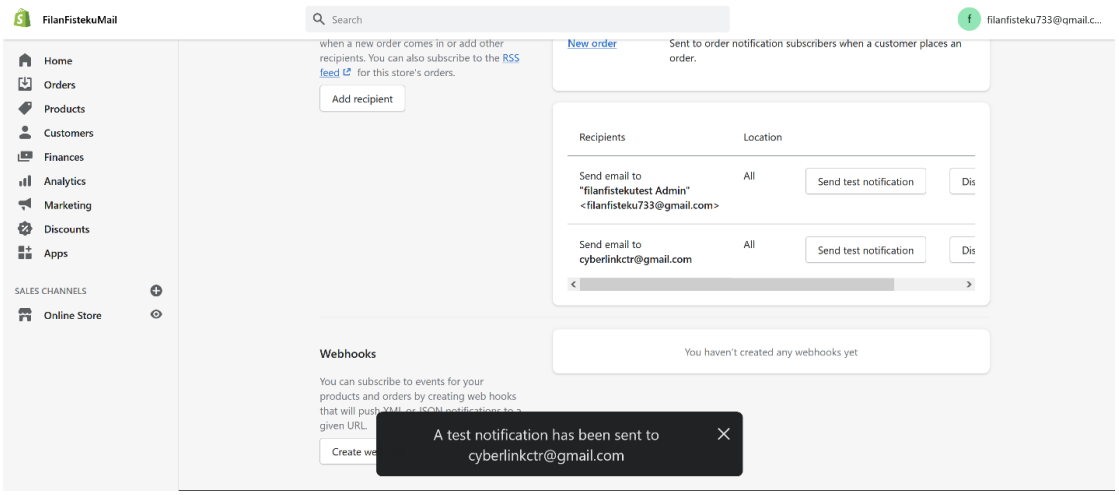


Figura 7. Regjistrimi i klientit për njoftime dhe dërgesa e sulmit

(Burimi: https://filanfistekutest.myshopify.com/admin/settings/notifications)

Më poshtë shohim se si vie emaili direkt në telefon.

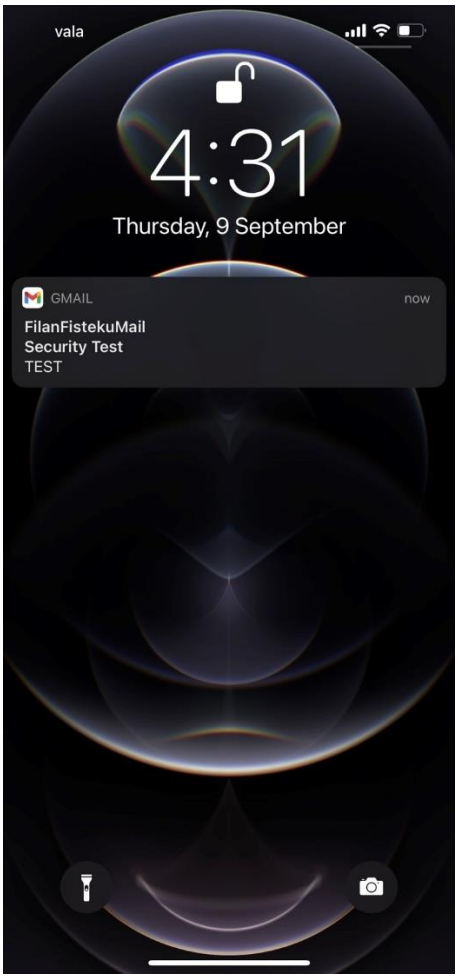


Figura 8. Mesazhi vie në telefon

(Burimi: iPhone Screenshot)

Siç e shohim email-i ka ‘name’ të kostumizuar. Dhe kur hapim email-in shohim se ka enkriptim dhe po ashtu ka nje email domain të cilin e kemi marrë pa pasur nevojë të e verifikojmë apo ta blejmë.

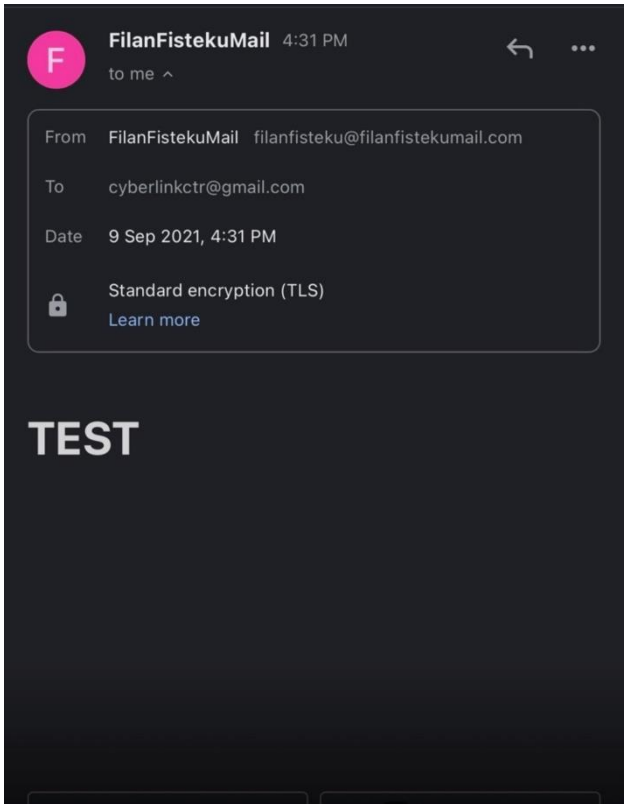


Figura 9. Analiza e mesazhit.

(Burimi: iPhone Screenshot)

Tani e kuptojmë se hakerët kanë arritur të parakalojnë edhe këto masa sigurie. Po ashtu ky lloj i sulmit është një sulm i cili ka shanca rreth 50% më shumë të ketë sukses për shkak se arrin të manipulojë njerëzit duke i bërë të mendojnë se emaili dërgues është email legjitim. Kjo email mund të dallohet se është “phishing” vetëm nëse shikohet detajisht se cila është platforma që përdoret për dërgimin e email-ave, përndryshe, është njëra ndër metodat më të avancuara ndonjëherë.

6. SI TË MBROHEMI NGA PHISHING

"Phishing-u" po përdoret çdo ditë e më shumë. Kjo na bën të kuptojmë që duhet të jemi të gatshëm të mos biem pre e këtyre sulmeve. Njëra ndër gjërat që duhet te merret parasysh sa më shpejt është të krijohet nje rregullore ndërkombëtare ku vetëdijesimi i të gjithë njerëzve nga fëmijët nëpër institucione të edukimit e deri tek drejtorët ekzekutiv të kompanive të bëhet i detyrueshëm. Përveç kësaj, më poshtë kemi edhe një listë të disa pikave qe mund të përforcojnë mbrojtjen nga "phishing".

1. Të shikohet kush ka dërguar E-mailin apo tekstin.
2. Të mos klikohet në link nëse email-i vjen nga nje burim jo i besueshëm.
3. Nëse klikohet ne link, te shikohet i gjithë Domaini për ndonjë karakter me shume ose me pak.
4. Spam Filters tek E-mails, E-mail Serverët apo edhe Ueb Serveret.
5. Të shikohet se a ka gabime drejtshkrimore ne E-mail.
6. Të shikohet se mos ka ndonjë kriptim ne tekst i cili është i ndryshëm nga UTF-8.
7. Asnjë kompani nuk e kërkon passwordin tuaj.

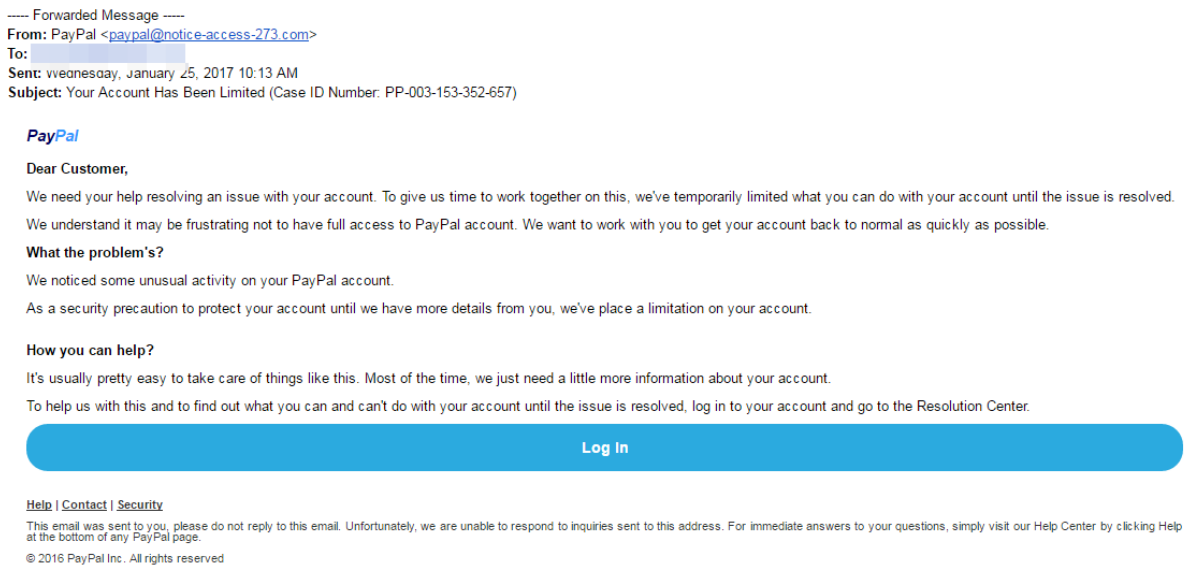
Duke ditur edhe se si të rritim mbrojtjen, gjithmonë ekziston pyetja se si të detektojmë një email "phishing" dhe po ashtu kemi bërë një përmbledhje të shkurtë më poshtë.

Mesazhi nuk dërgohet nga një domain privat

Të gjitha organizatat legjitime kanë domain emailat e tyre private të rezervuara. Nuk ekziston ndonjë mënyrë ku këto organizata do dërgojnë një email me email domain siç është '@gmail.com'. Shumica e organizatave apo bizneseve, e kanë domainin e emailit të tyre personal. Mund ta marrim si shembull nëse domaini është 'www.filanfisteku.com', atëherë emailat të cilët kjo kompani do dërgojë do janë filan@filanfisteku.com. Por problemi që shfaqet

është tek njerëzit, për shkak se shumica nuk e shikojnë dërguesin e emailit por shikojnë titullin apo subjektin që kanë përpara.[47]

Më poshtë kemi një shembull të një sulmi "phishing"i cili është një ndër sulmet e avancuara që kemi përmendur më herët. Nëse e analizojmë tërë imazhin e kuptojmë se i vetmi lëshim është pjesa e dërguesit të emailit, përndryshe, i tërë sulmi duket si një email legjitime nga paypali.



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

Figura 10. Një "phishing"email me temë paypal

(Burimi:https://www.welivesecurity.com/2017/01/27/paypal-users-targeted-sophisticated-new-phishing-campaign/)

Kjo e-mail është shumë problem që të dallohet se është mashtrim. Siq e shohim, në fillim gjendet logoja e paypalit dhe pastaj vazhdon me 3 pika kryesore: 1. Prezantimi, 2.Sqarimi i problemit, 3.Aksioni që duhet ndërmarrë, kurse në fund e ka pjesën fundore e cila duket si një kopje e emailave të cilat i dërgon paypal. Një person normal shumë lehtë mund të bie pre e kësaj teknike për shkak se jo çdokush i jep rëndësi detajeve të vogla si kjo.

Por çka ne duam të bëjmë është të kuptojmë se si të dallojmë këtë email dhe ta dimë se është "phishing". Janë 3 elemente që na lejojnë të kuptojmë se ky nuk është e-mail legjitim.

[47] Luke Irwin, 5 ways to detect a "phishing"email, Qershor 2020, tek https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email (qasur për herë të fundit më 10 Shtator 2021)

1. Dërguesi i emailit nuk e përdor domain email-in e paypalit por përdor domain emailin notice-accesss-273, i cili nuk është domain email-i i paypal.
2. "**What the problem's?**" është gabim drejtshkrimor dhe nuk është i shkruar në gjuhë zyrtare të cilën një kompani serioze si paypal duhet ta përdorë. Mënyra korrekt për t'u shkruar do ishte "**What the problem 'is'**".
3. Butoni Log in. Siq shihet butoni Log in është shumë i gjatë dhe normalisht nuk do duhej të ishte kaq i gjatë. Zakonisht emailat që dërgohen e kanë këtë buton shumë më të optimizuar.

Në këtë email nuk patëm mundësinë të gjejmë shumë gabime por disa nga gabimet që shumica e hakerëve bëjnë janë këto.

1. Drejtshkrimi – Ku shumica e hakerëve nuk kanë një fjalor të pasur dhe nuk dinë të shkruajnë me gramatikë. Po ashtu për shkak se shumica e emailave kanë "spam" filterët të cilët dërgojnë në spam emailat e dyshimtë hakerët detyrohen të shtojnë apo heqin shkronja nga fjalë të ndryshme të cilat mund të detektohen nga filterët ku është shumë e lehtë të detektohen këto lëshime.
2. Dërgimi në sasi të madhe – Shumicën e rasteve hakerët marrin një listë të email-ave dhe e dërgojnë "phishing-un" e njëjte. Dhe mundësia për dërgim të gabuar është shumë e madhe. P.sh. hakeri u ka dërguar një "phishing" për të ndërruar passwordin e llogarisë netflix dhe ka mundësi që 20 nga 100 persona nuk kanë llogari të netflix, me një fjalë, sulmi shkon huq dhe detektohet menjëherë nga ata persona.
3. Aksion i menjëhershëm – Shumica e phishing-ave kërkojnë një aksion të menjëhershëm, e cila automatikisht shpie në dyshimë, dhe ato dyshime e bëjnë shumë më të lehtë të detektohet se emaili është phishing

Edhe duke ditur se si të mbrohemi dhe detektojmë një sulm të llojit të tillë, prapë nuk është mjaftueshëm. "phishing" ende është një taktikë shumë efektive për të marrë qasje në llogaritë personalë të njerëzve. Dhe, siç e pamë tek rasti i studimit me shopify, hakerët vetëm po vazhdojnë ta vështirësojnë punën e detektimit të këtyre sulmeve. Por kjo nuk do të thotë që jemi total të pambrojtur. Duhet që rregullisht të marrim masa për rritjen e sigurisë dhe vetëdijesimit të te gjitha entiteteve që potencialisht mund të bien pre e "phishing". Praktikë e mirë është që të edukohet i tërë stafi rregullisht për vetëdijesim të sigurisë në mënyrë që të detektohet një sulm

“phishing” në mënyrë natyrale dhe të bëhen kampanja vetëdijesuese të organizuara nga vetë shteti që te edukohen të gjithë njerëzit.

7. KONKLUZION

Po kuptohet se numri i sulmeve çdo dite po vjen e po shtohet. Kjo na tregon se ne jemi gjithmonë një hap prapa hakerëve. Po ashtu “phishing”po shkon duke evoluar gjithmonë duke iu afruar një imitimi te faqeve origjinale mbi 90%. E vetmja qe na ka mbetur është te krijohet një rregullore e cila i mëson të gjithë se çfarë është “phishing” dhe se si ta evitojmë një sulm të suksesshëm “phishing”. Po ashtu duhet të bëhet e detyrueshme testime të rregullta të sigurisë çdo 3 muaj në mënyrë që metodat e mbrojtjes të jenë gjithmonë të përditësuara. Duhet që të kuptohet se është vitale që inxhinierët e sigurisë kibernetike të fillojnë të krijojnë teknika të reja të dhe të mundohen që të jenë në një hap me hakerët. Nuk është e mjaftueshme që vetëm të dinë mënyra se si të mbrohen, por duhet që të ketë inxhinierë që e shfrytëzojnë kreativitetin e tyre që të krijojnë po ashtu teknika të reja sulmi në atë mënyrë që kur hakerët ti zbulojnë ato, inxhinierët të jenë një hap me ta së paku. Vetëdijesimi dhe siguria kibernetike nuk është në nivelin e duhur, jo vetëm lokalisht por edhe në të gjithë botën. Një botë ku shumica e sulmeve bazike të “phishing”rezultojnë si sulme të suksesshme, është një botë e cila nuk i kushton rëndësi sigurisë kibernetike. Nëse aplikohen në të gjitha entitetet trajnimet e ndryshme sa i përket vetëdijesimit të sigurisë, dhe po ashtu trajnime ku ekspertet vetëm u tregojnë entiteteve se çfarë rreziqesh ekzistojnë, atëherë brenda pak vitesh ekziston mundësia që një sulm “phishing”i avancuar të mos ketë sukses për shkak se “phishing”e shfrytëzon ngutinë e natyrës humane dhe faktin që jo të gjithë u japin rëndësi detajeve të vogla. “phishing”mund të ndalohet dhe nuk do edhe aq shumë punë, vetëm përkushtim dhe dëgjim nga ana e njerëzve.

8. REFERENCAT

Check Point Research . (2018). *Check Point Research Security Report 2018.*

NTT. (2018). *NTT Security Global Threat Intelligence Report* .

Anti-”phishing”Working Group (APWG). (2020). *Anti-”phishing”Working Group (APWG) Report* .

Core Security. (a.d.). *How “phishing”Has Evolved and Three Ways to Prevent Attacks*. Gjetur në CoreSecurity.com: https://www.coresecurity.com/blog/how-phishing-has-evolved-and-three-ways-prevent-attacks

EY Global. (a.d.). EY Global Information Security Survey 2018. 2018.

Felix, J. &. (1987). *System Security: A Hacker's Perspective.* Interex Proceedings.

Hewitt, K. (2021, 5). *12 Types of “phishing”Attacks and How to Identify Them*. Gjetur në Securityscorecard.com: https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them

Jones, C. (2021, 7). *50 “phishing”Stats You Should Know In 2021*. Gjetur në expertinsights.com: https://expertinsights.com/insights/50-phishing-stats-you-should-know/#The%20Frequency%20Of%20Phishing%20Attacks

Packet Labs . (a.d.). *Cybersecurity Statistics 2021*. Gjetur në Packetlabs.net: https://www.packetlabs.net/cybersecurity-statistics-2021/

“phishing”Box. (a.d.). *“phishing”Facts*. Gjetur në www.phishingbox.com: https://www.phishingbox.com/resources/phishing-facts

“phishing”. (a.d.). *History Of “phishing”.* Gjetur në “phishing”. org: https://www.”phishing”. org/history-of-”phishing”

Phishing, G. –G.—C. (2005, 12 30). *GP4.3 – Growth and Fraud — Case #3 – "phishing".* Gjetur në Financial Cryptography: https://financialcryptography.com/mt/archives/000609.html

Symantec Internet Security . (2016). *Symantec Internet Security Threat Report.*

Symantec Internet Security. (2019). *Symantec Internet Security Threat Report (ISTR)* .

Verizon . (2016). *Verizon Data Breach Investigations Report (DBIR)* .

Verizon . (2019). *Verizon Data Breach Investigations Report (DBIR)* .

Verizon. (2017). *Verizon Data Breach Investigations Report (DBIR)* .

Verizon. (2018). *Verizon Data Breach Investigations Report (DBIR).*