AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

NDËRGJEGJËSIMI NDAJ INXHINIERISË SOCIALE: MBRONI VETEN NË EPOKËN DIGJITALE

SHEMBULL I INXHINIERISË SOCIALE NË JETËN REALE

HAKER ME AFTESI SOCIALE

David njihet si një inxhinier social, ose si një haker njerëzor. Arti i tij është të bindë njerëzit të ndajnë informacione që nuk duhet të ndajnë. Disa e përdorin këtë teknikë për aktivitete të paligjshme. Por në rastin e Davidit ai punësohet dhe paguhet nga kompanitë për të testuar për dobësi.

KEVIN MITNICK: KUMBARI I INXHINIERISË SOCIALE

LIBRI I TIJ "ARTI I MASHTRIMIT" ËSHTË NJË BURIM I MIRË.

- (2002) The Art of Deception: Controlling the Human Element of Security
- (2005) The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers
- (2011) Ghost in the Wires: My Adventures as the World's Most Wanted Hacker
- (2017) The Art of Invisibility

./WHOAMI

JETMIR RAJTA – CEH | BLUE TEAM | CAPACITY BUILDING | DATA ANALYSIS

6 vite në IT dhe Siguri Kibernetike

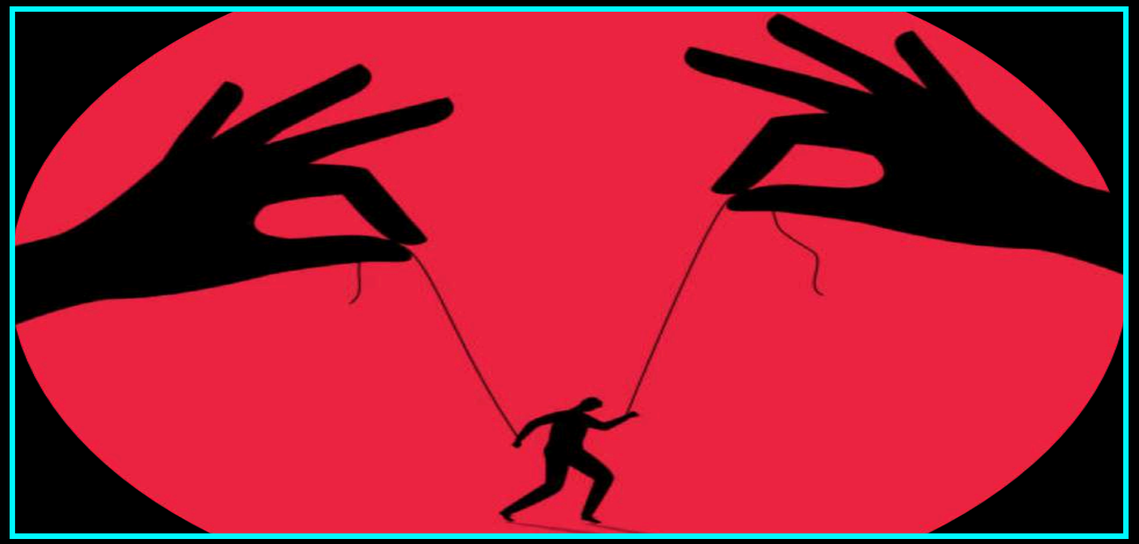
Certifikuar nga: EC Council si Certified Ethical Hacker, Pjesë e 1% botëror në TryHackMe.

Arsimi: ICT, Shkenca Politike, Marrëdhënie Ndërkombëtare, Edukim Ushtarak dhe Siguri Kibernetike.

Shërbej si specialist i Sigurisë Kibernetike në Autoritetin Kombëtar për Sigurinë Kibernetike (AKSK).

I përfshirë në hackathone, TTX, Cyber Drills, CTF dhe workshop-e për ngritjen e kapaciteteve.

ÇFARË ËSHTË INXHINIERIA SOCIALE?



Inxhinieria Sociale është një vektor sulmi që mbështetet shumë në ndërveprimin njerëzor dhe shpesh përfshin mashtrimin e njerëzve për të thyer procedurat normale të sigurisë.

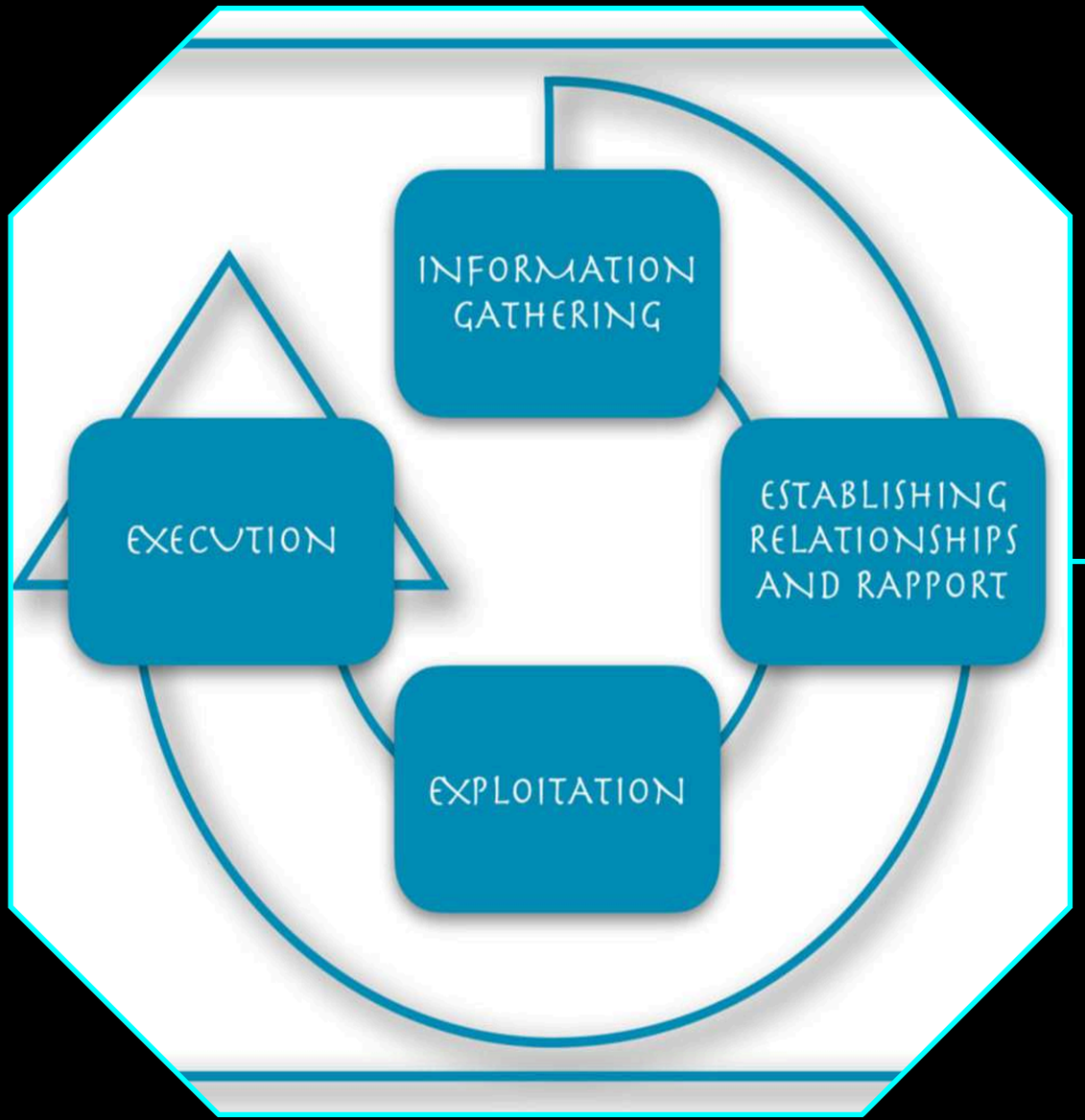
INXHINIERIA SOCIALE ËSHTË ARTI I TRE GJËRAVE:

- Manipulimit
- Ndikimit
- Mashtrimit

CIKLI I SULMIT

Ekziston një sekuencë e parashikueshme me katër hapa për sulmet e inxhinierisë sociale, të referuara zakonishtsi cikli i sulmit.
Cikli i sulmit përfshin:

- mbledhjen e informacionit,
- krijimin e marrëdhënievedhe raporteve,
- shfrytëzimindhe
- ekzekutimin.



KARAKTERISTIKA E NJË SULMI TË INXHINIERISË SOCIALE

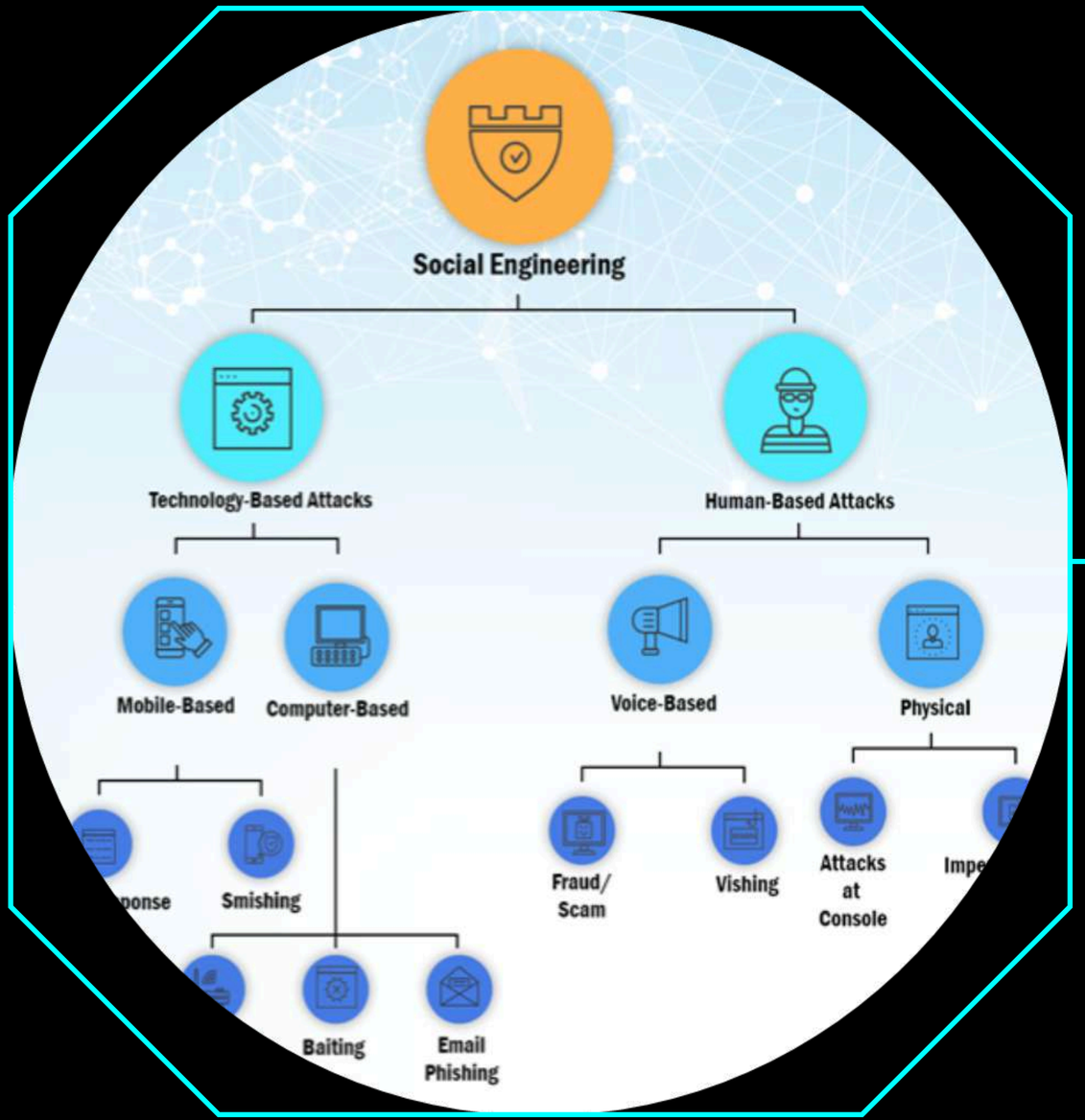
Inxhinierët socialë mbështeten në emocionet njerëzore për të motivuar njerëzit të bëjnë atë që ata duan. Me fjalë të tjera, këta kriminelë përdorin manovra delikate psikologjike për të fituar besimin e një personi dhe më pas e shfrytëzojnë atë.

QËLLIMET:

- Paratë
- Egoja
- Hakmarrja
- Shkak
- Argëtim
- Njohuri

LLOJET E ZAKONSHME TË INXHINIERISË SOCIALE

- Me bazë njeriun
- Me bazë teknologjinë



METODAT E BAZUARA NË NJERËZ

- Imitimi
- Frika
- Krijimi i konfuzionit
- Mund t'ju ndihmoj?
- A mund të më ndihmosh?
- Ndërtimi i besimit
- Kërkoni dhe do t'ju jepet kërkoni dhe do të gjeni.
- Zhytja në kosh/Dumpster Diving

METODAT E BAZUARA NË TEKNOLOGJI

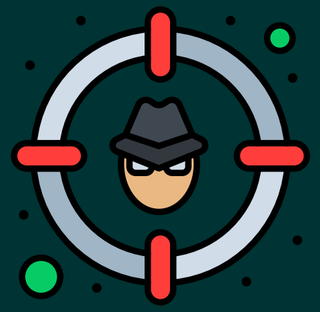
- Dritaret kërcyese – Pop Up Windows
- Bashkëngjitjet e email-it.
- Pishing/Smishing
- Faqet e internetit të phishing
- Pajisje USB
- Key Loggers

TEKNIKA PËR BINDJE

- Ndërtimi i besimit dhe marrëdhënieve
- Inkuadrimi i Mesazhit
- Përshtatja e Qasjes
- Dorëzimi

INXHINIERIA SOCIALE NUK MUND TË BLLOKOHET VETËM NGA TEKNOLOGJIA.

- Elementi njerëzor
- Manipulimi psikologjik
- Rrjetet sociale
- Sulmet e targetuara
- Kërcënimet e brendshme

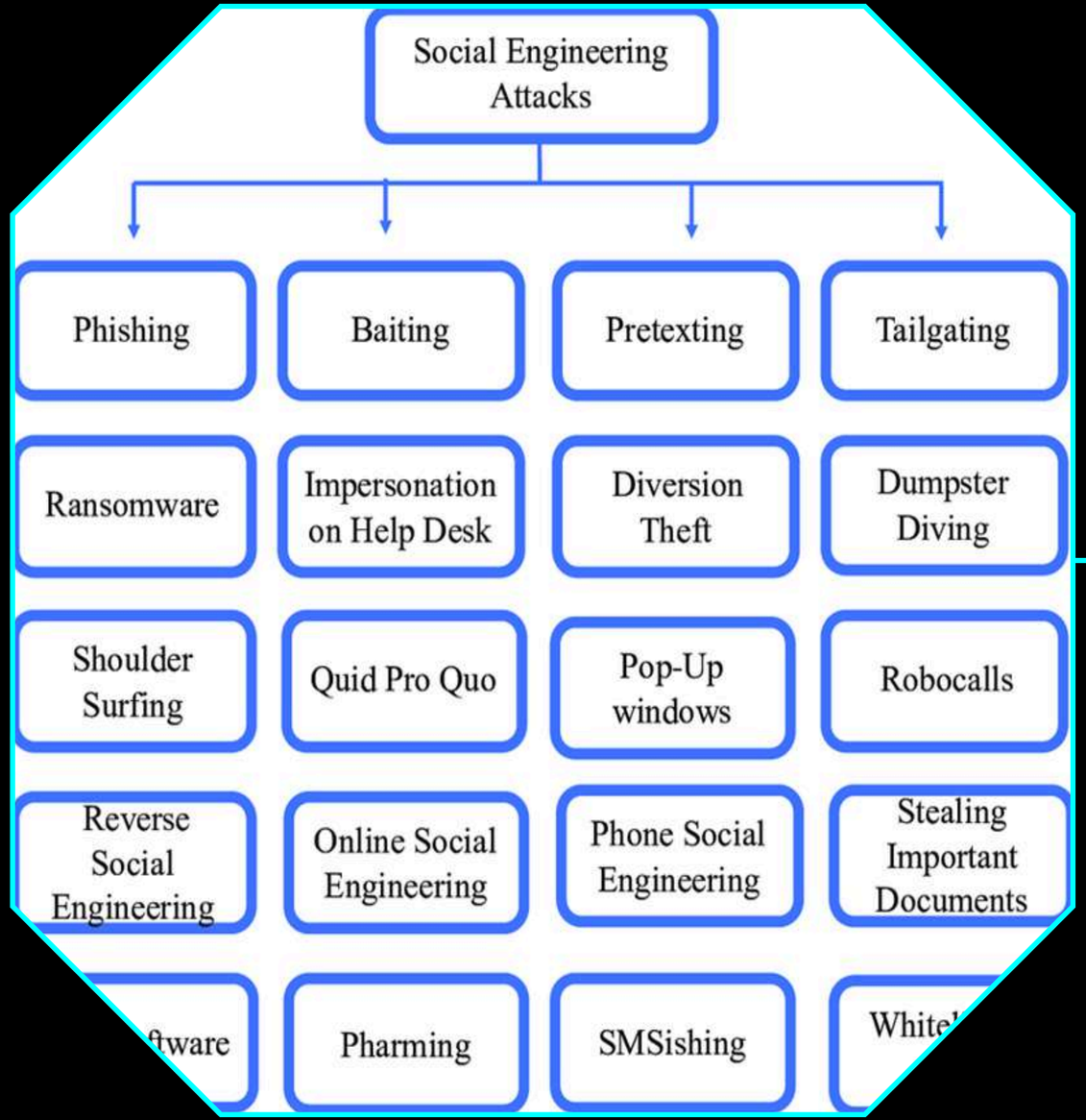


SULMET TIPIKE:

- Shërbimi ndaj klientit
- Personi i dërgesave/shërbimeve postare
- Telefon/Vishing
- Suport Teknik

DISA NGA METODAT E SULMEVE TË INXHINIERISË SOCIALE

- Dumpster Diving
- Shoulder Surfing
- Baiting/Karremi
- Vishing
- Phishing
- Whaling



DUMPSTER DIVING

- Faturat e Kartës së Kreditit
- Faturat e paguara
- Emaile të printuara
- Fjalëkalime
- Numra telefoni
- Emra
- Të dhënat e shpenzimeve

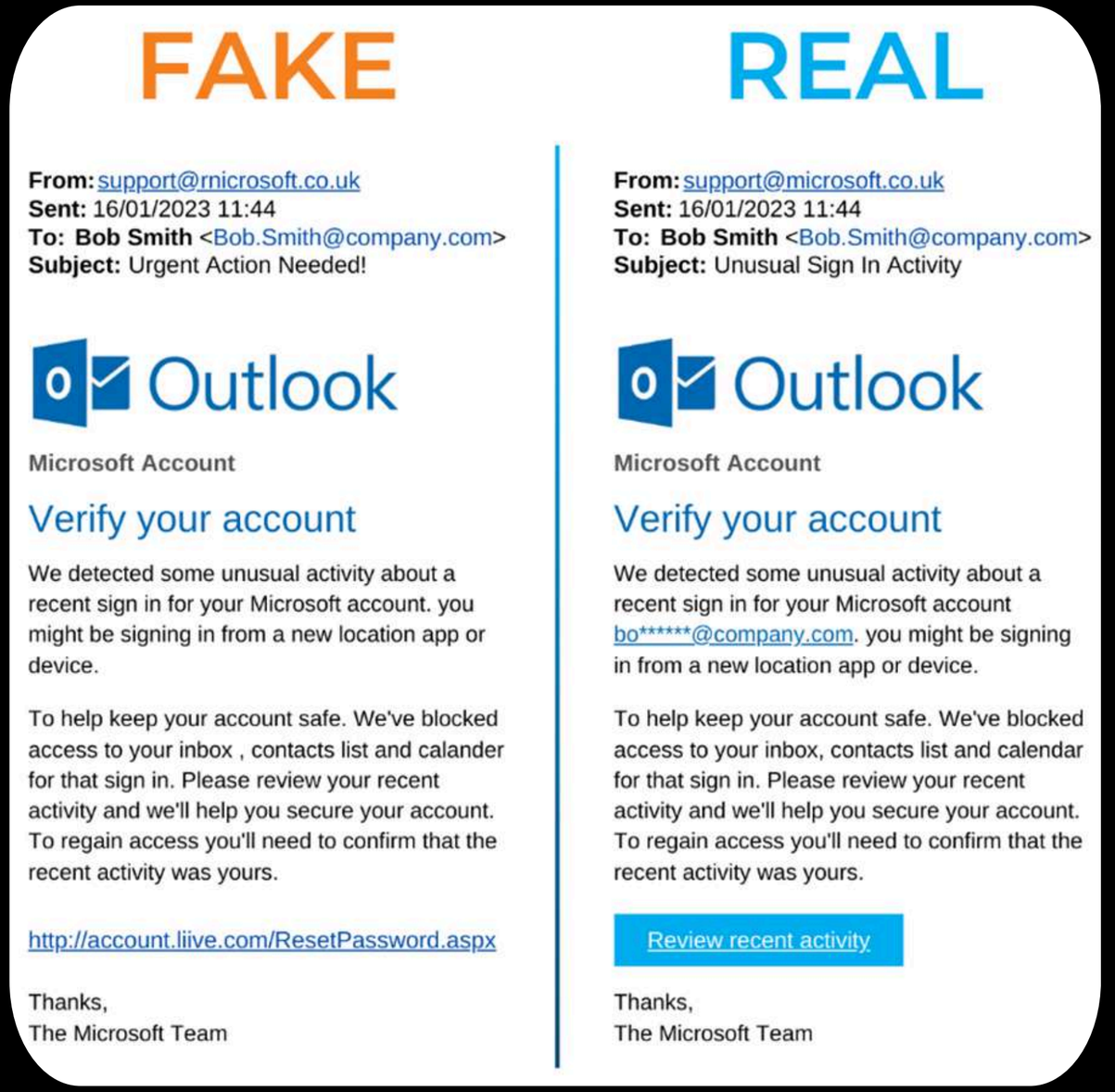
SHOULDER SURFING

Një sulm me lundrim mbi shpatullah shpjegon një situatë kur sulmuesi mund të shikojë fizikisht ekranet e pajisjeve dhe tastierën e shtypjes së fjalëkalimit për të marrë informacion personal, d.m.th. Metoda e këtij lloj sulmi kërkon që hakeri (sulmuesi) të jetë fizikisht afër viktimave që sulmi të ketë sukses.

EMAIL-ET E PHISHING

Një nga format më të zakonshme të inxhinierisë sociale janë emailet e phishing. Ata shpesh duket se vijnë nga burime të besueshme, si bankat, faqet e mediave sociale, apo edhe punëdhënësi juaj.

Zakonisht, emailet përdorin taktika të frikësimit ose krijojnë një ndjenjë urgjence për t'ju detyruar të ndërmerrni veprime urgjente.

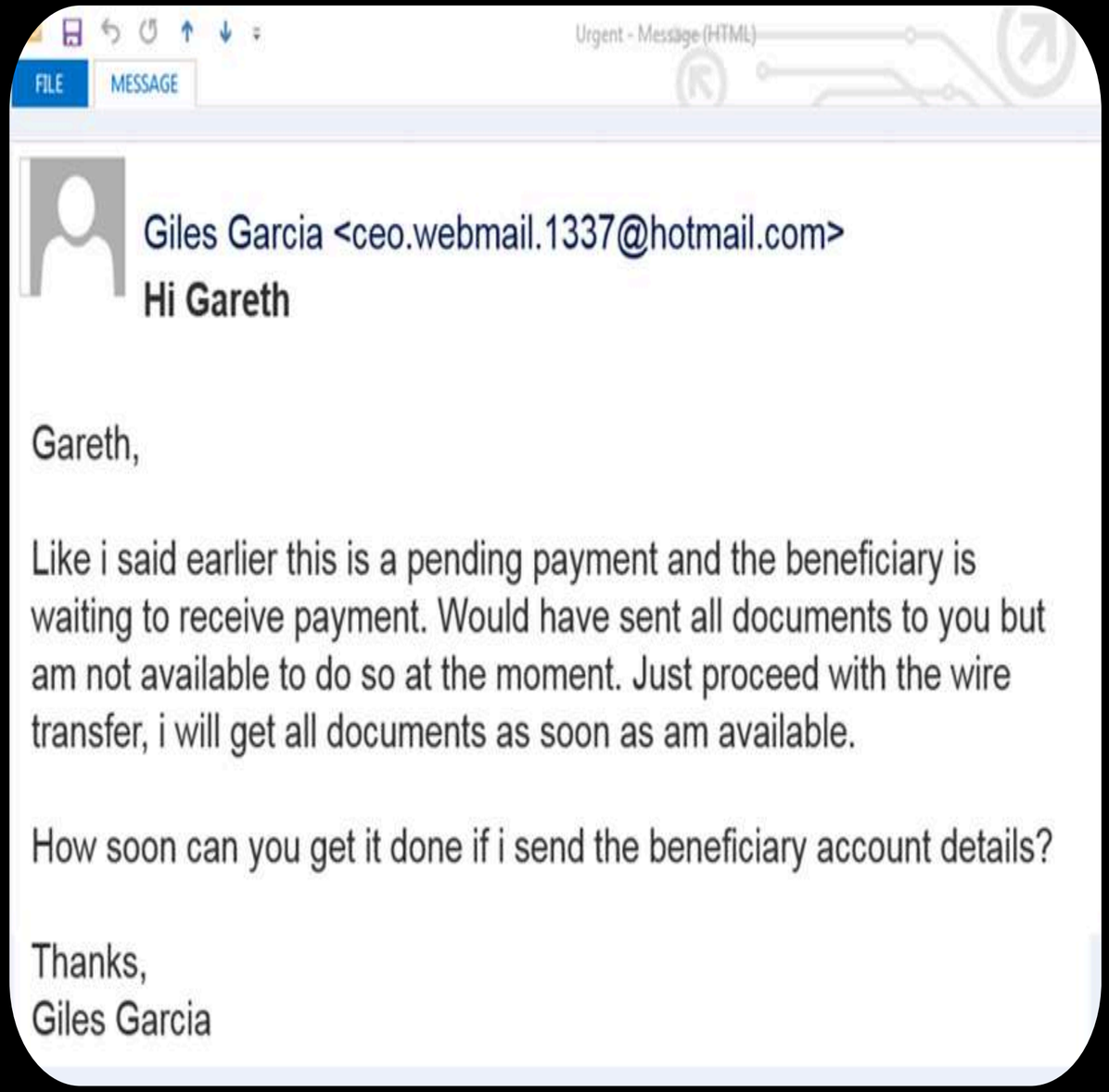


SPEAR PHISHING

Spear phishing është një mashtrim me email ose komunikime elektronike që targeton/synon një individ, organizatë ose biznes të caktuar.

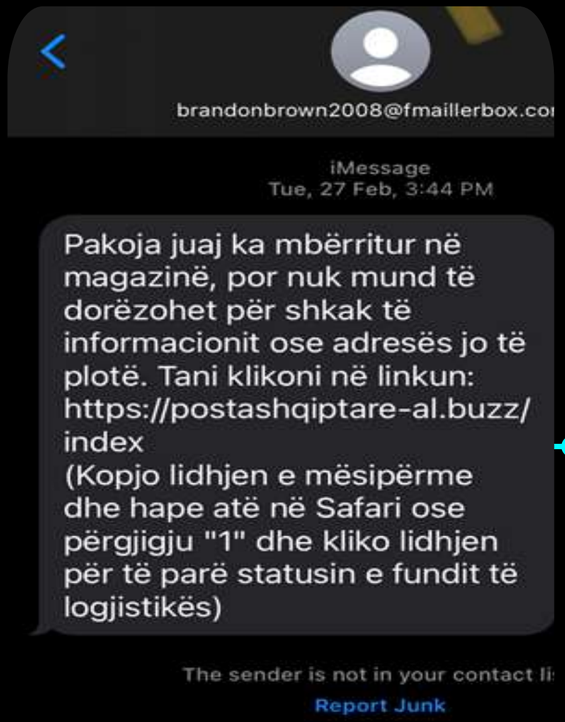
WHALING

Një sulm i whaling, i njohur gjithashtu si gjueti për balena, është një lloj specifik sulmi phishing që synon punonjësit e profilit të lartë, si shefi ekzekutiv ose shefi financiar, për të vjedhur informacione të ndjeshme nga një kompani.



SMISHING

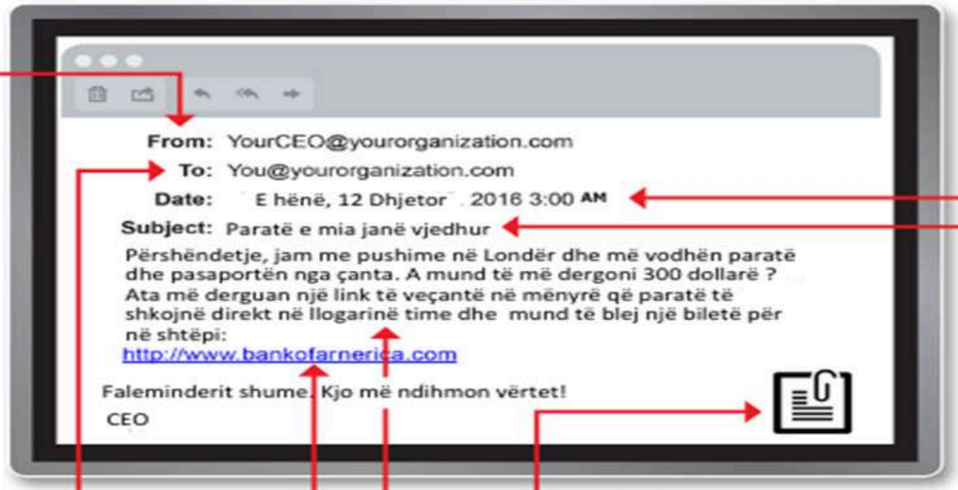
Smishing është një lloj sulmi phishing që përdor inxhinierinë sociale për të marrë informacione personale për dikë nëpërmjet mesazheve me tekst.



Inxhinieria Sociale - Red Flags

DËRGUESI

- Nuk e njihni adresën e emailit të dërguesit si dikë me të cilin **komunikoni zakonisht**.
- Ky email është nga dikush **jashtë organizatës dhe nuk është i lidhur me përgjegjësitë e punës**.
- Ky email është dërguar nga **dikush brenda organizatës** ose nga një klient, shitës ose partner dhe është **shumë i pazakontë**.
- A është adresa e emailit e dërguesit nga një **domain i dyshimtë**? (si për shembull: mikorsoft-support.com)
- **Nuk e njihni personalisht dërguesin** dhe nuk është nga dikush që keni besim.
- **Nuk keni një marrëdhënie biznesi** dhe as ndonjë komunikim të mëparshëm me dërguesin.
- Ky është një **email i papritur ose i pazakontë** me një **link të integruar ose një dokument të bashkëngjitur** nga dikush me të cilin nuk keni komunikuar kohët e fundit.



DATA

- A keni marrë një email që normalisht duhet ta merrnit gjatë orarit të rregullt të punës, por ai u **dërgua në një orë të pazakontë** si ora 3 e mëngjesit?

SUBJEKTI

- A keni marrë një email me një subjekt që është **e parëndësishme** ose **nuk përputhet** me përmbajtjen e mesazhit?
- A është mesazhi i emailit një përgjigje për diçka që **nuk e keni dërguar apo kërkuar kurrë**?

PËR

- Jeni vendosur në CC në një email dërguar një ose më shumë njerëzve, por **personalisht nuk i njihni** personat të cilëve u është dërguar.
- Keni marrë një email që iu dërgua gjithashtu një **përzierjeje të pazakontë njerëzish**. Për shembull, mund t'i dërgohet një grupi të rastësishëm njerëzish në organizatën ku punoni, mbiemrat e të cilëve fillojnë me të njëjtën shkronjë, ose një list e gjatë me adresa të dyshimta.

BASHKËNGJITJET

- Dërguesi ka përfshirë një dokument të bashkëngjitur në email që **nuk e prisnit** ose që **nuk ka kuptim** në lidhje me mesazhin e emailit. (Ky dërgues nuk iu dërgon zakonisht këtë lloj bashkëngjitjeje.)
- Shihni të bashkëngjitur një email me një lloj **skedari ndoshta të rrezikshëm**. I vetmi lloj skedari që është **gjithmonë i sigurt për t'u klikuar është një skedar .txt.**

HYPERLINKS

- Vendosni mouse-in mbi një link që shfaqet në mesazhin e emailit, por shihni që **adresa e linkut të drejton në një tjetër website**. (Ky është një ***sinjal kritik paralajmërimi***.)
- Ju është dërguar një email që ka vetëm **hiperlinqe të gjata pa informacion të mëtejshëm**, dhe pjesa tjetër e emailit është plotësisht bosh.
- Ju është dërguar një email me një **link që ka gabime drejtshkrimore** të një faqeje të njohur interneti. Për shembull: www.bankofarnerica.com - ku shkronja "m" është krijuar si bashkim i dy karaktere - "r" dhe "n".

PËRMBAJTJA

- A është duke iu kërkuar dërguesi të klikoni në një link ose të hapni dokument të bashkëngjitur për të **shmangur një pasojë negative** ose **për të fituar diçka me vlerë**?
- A është emaili **jo i zakonshëm**, apo ka **gabime gramatikore** dhe **drejtshkrimore**?
- A është duke iu kërkuar dërguesi të klikoni një link ose të hapni një dokument të bashkangjitur që **duket i çuditshëm** ose **i palogjikshëm**?
- A keni **një ndjenjë të pakëndshme** lidhur me kërkesën e dërguesit për të hapur një dokument ose për të klikuar një link?
- A është emaili duke iu kërkuar të shikoni **një foto kompromentuese ose të sikletshme** të vetes suaj ose të dikujt që njihni?

PËRTEJ EMAILEVE DHE TELEFONATAVE: PRETEKSTI DHE BAITING (KARREMI)

- Preteksti: Arti i tregimit të rremë
- Baiting/Karremi: Ofrimi i marrëveshjeve ose promovimeve në dukje tërheqëse.

BAITING (KARREMI)

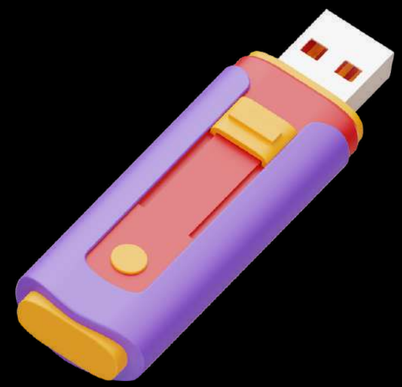
Karremi/Baiting është një lloj sulmi ku një haker do të përdorë një premtim ose shpërblim të rremë për të mashtruar viktimat dhe për të vjedhur informacionin e tyre të ndjeshëm duke infektuar sistemin e tyre me malware.

KARREM FIZIK ME NJË PAJISJE:

Eksperiment: Në një eksperiment të kontrolluar të kryer nga Universitetii Miçiganit, Universitetii Illinois dhe Google, rreth 300 pajisje flash USB u lanë si karrem në 30 vende të ndryshme.

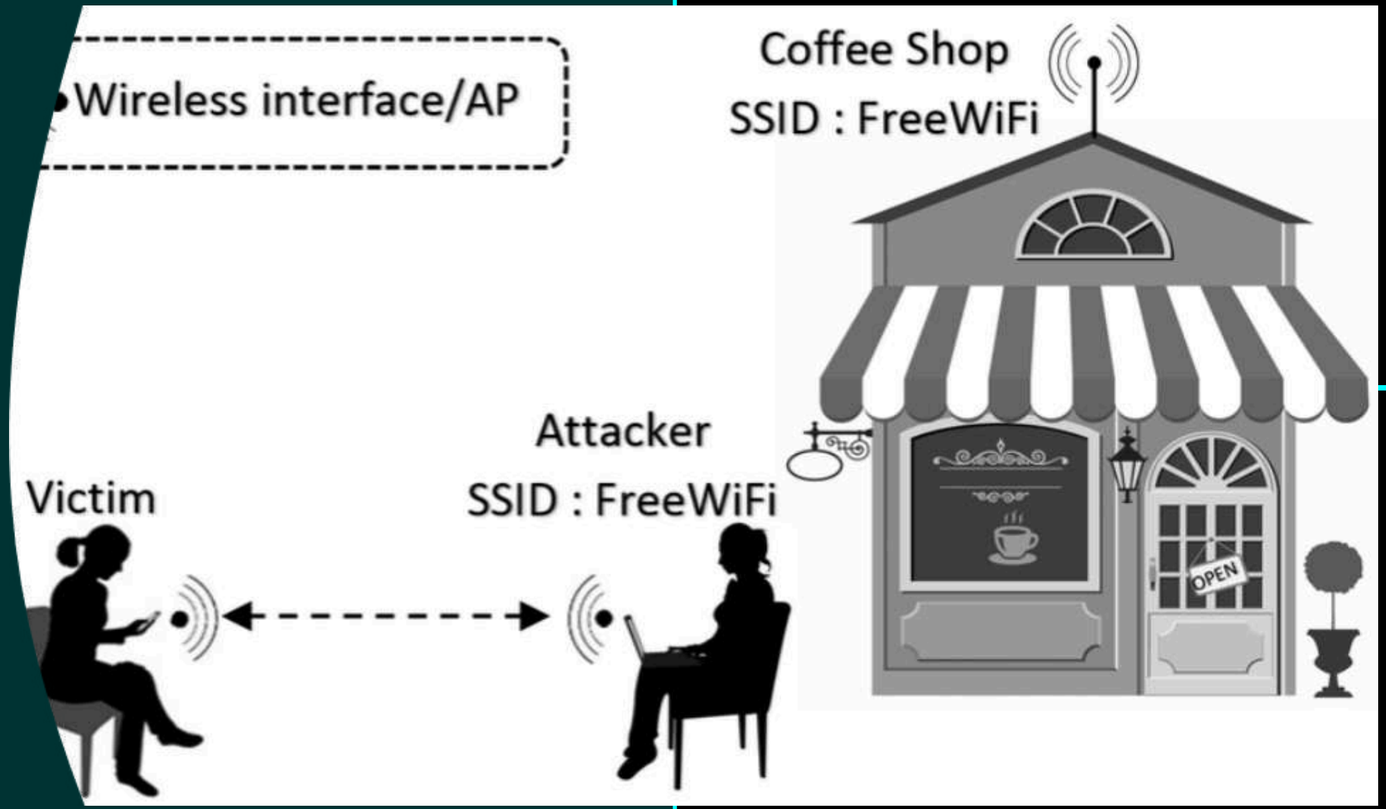
Rezultati: U zbulua se 45%-98% e njerëzve lidhin pajisjet USB që gjejnë. Midis tyre, 68% e përdoruesve deklaruan se nuk morën masa paraprake kur lidhnin pajisjen. Ndër ata që menduan për masat e sigurisë, 10 (16%) skanuan flash drive duke përdorur softuer antivirus, dhe 5 (8%) besonin se sistemi i tyre operativose softueri i sigurisë do t'i mbronte. 5 të tjerë (8%) përdorën burimet e universitetit për të mbrojtur pajisjet e tyre personale.

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive



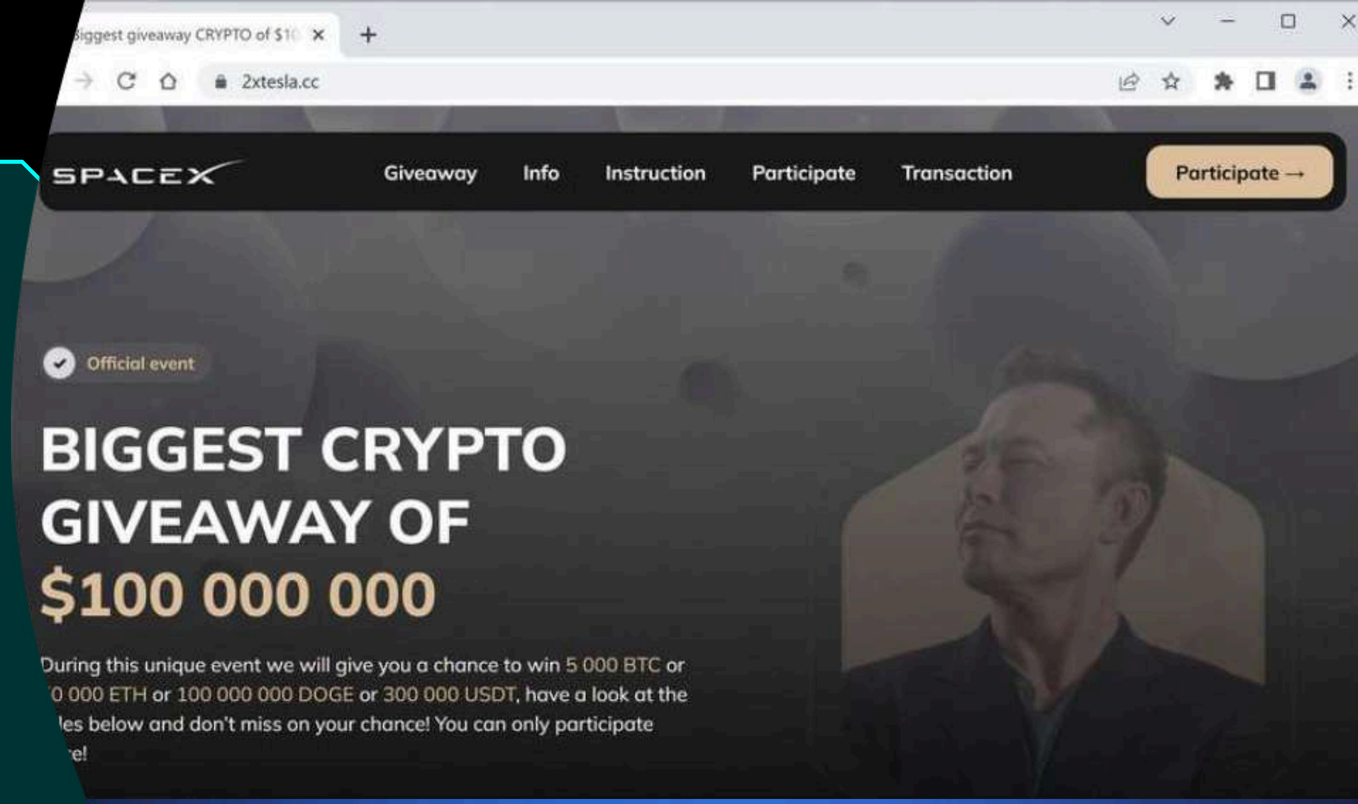
QUID PRO QUO

Diçka për diçka



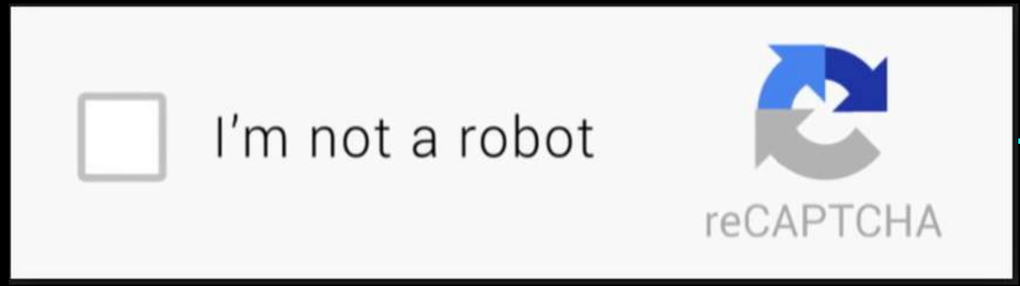
KUIZET NË FACEBOOK

DHURATA TË KRIPTOMONEDHAVE



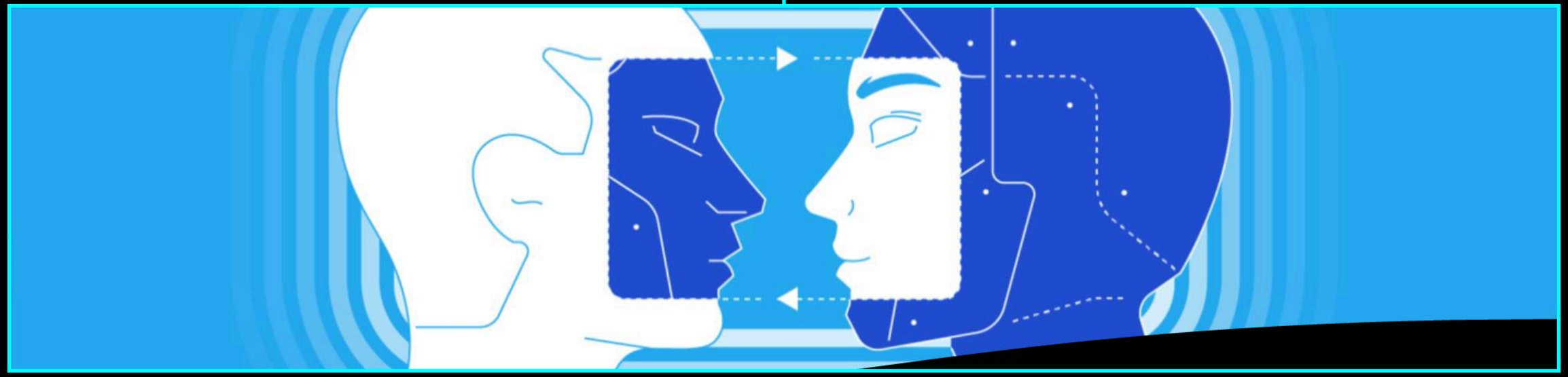
KODET QR DHE TESTET CAPTCHA: MASHTRIME TË REJA NË NJË EPOKË DIXHITALE:

TË SKANOSH APO TË MOS SKANOSH?



SI TË IDENTIFIKONI NJË INXHINIER SOCIAL?

- Nuk jep informacion kontakti
- Kërkon gjithmonë informacione të ndaluara
- Aktivitete të nxituara
- Përdor elementin Frikë
- Vëzhgoni për gabime të vogla drejtshkrimore



ZBUTJA/SHMANGIA E INXHINIERISË SOCIALE

- Grirëse dokumentash/Shredder
- Politikat dhe procedurat
- Ndërgjegjësime
- Patchime të përditësuara dhe azhornim të Anti-Viruseve

KËSHILLA SI TË MBRONI VETEN TUAJ NË NIVEL PERSONAL

- Injoroni kërkesat për informacione personale; verifikoni drejtpërdrejt me kompaninë.
- Monitoroni historinë dhe ndryshimet e hyrjes në login.
- Mos ndani informacione personale në internet.
- Përdorni fjalëkalime unike, të forta; Mbi 14 karaktere.

KËSHILLA SI TË MBRONI VETEN TUAJ NË NIVEL ORGANIZATE

- Etiketoni emailet e jashtme me "EMAIL EXTERNAL".
- Monitoroni llogaritë për aktivitete të dyshimta.
- Përmirësimi i MFA-së; shmangni MFA-të e bazuar në email.
- Monitoroni hyrjet e privilegjuara për anomali.
- Ndaloni hyrjet anonime me VPN.
- Edukoni stafin për inxhinierinë sociale, phishing.
- Raportoni mesazhe të dyshimta.
- Vërtetoni thirrjet nga palët e treta.

PAKETA E INXHINIERISË SOCIALE

• Paketa e veglave të inxhinierisë sociale (SET) është një grup veglash të programuara në python, të cilat fokusohen vetëm në sulmin ndaj elementit njerëzor të testimit të depërtimit.

• SET u shkrua nga David Kennedy (ReL1K) dhe me shumë ndihmë nga komuniteti dhe ka inkorporuar sulme të paparë më parë në një grup veglash shfrytëzimi.

• Qëllimi kryesor është të simulojë sulmet inxhinierike sociale dhe të lejojë testuesin të testojë në mënyrë efektive se si mund të ketë sukses një sulm i targetuar.

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | D

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pw

https://aksk.gov.al/

FALEMINDERIT PËR VËMËNDJEN!