

Ndërgjegjësimi ndaj Inxhinierisë Sociale: Mbroni veten në Epokën Dixhitale

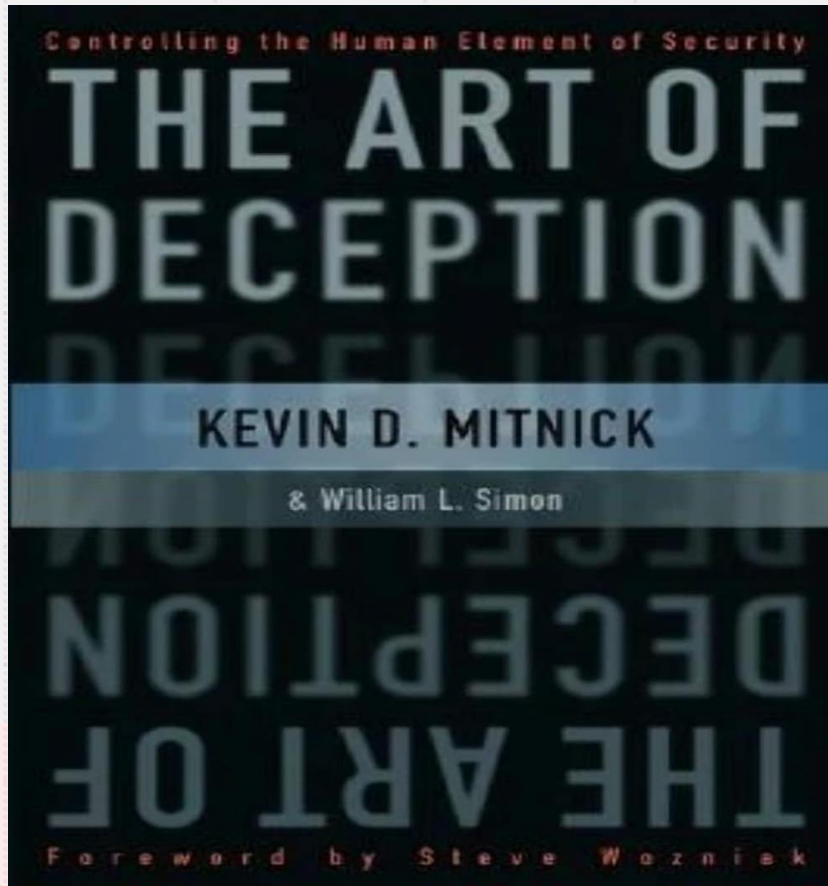
Autoriteti Kombëtar për
Certifikimin Elektronik dhe
Sigurinë Kibernetike




Shembull i inxhinierisë sociale në jetën reale



Kevin Mitnick: Kumbhari i Inxhinierisë Sociale



./whoami

 Jetmir Rajta - CEH | Blue Team | Capacity Building | Statistics

- Unë **NUK** jam një hacker, thjesht një analist i sigurisë kibernetike.
- 5 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 Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK).
- 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

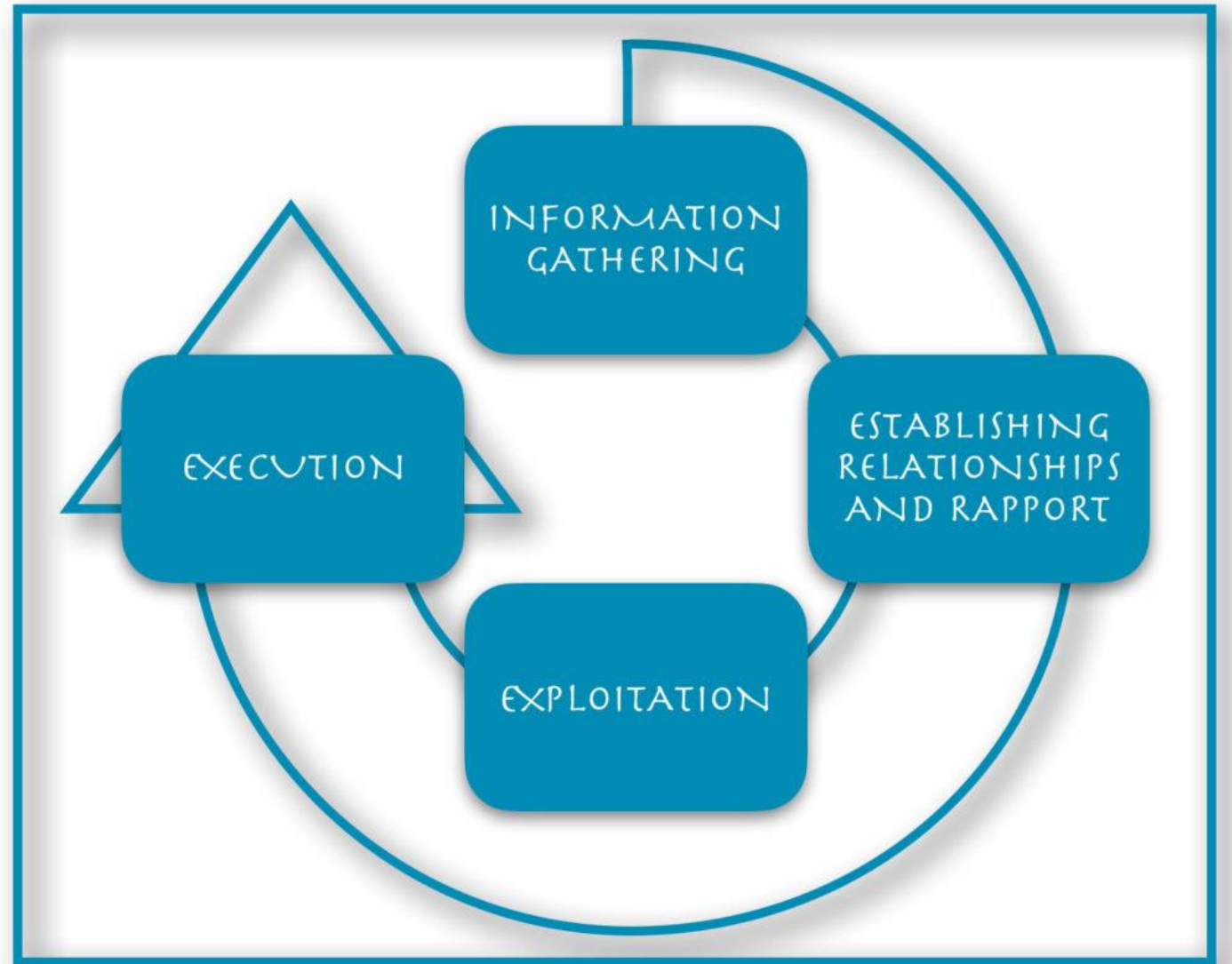


Cikli i Sulmit

Ekziston një sekuencë e parashikueshme me katër hapa për sulmet e inxhinierisë sociale, të referuara zakonisht si cikli i sulmit.

Cikli i sulmit përfshin:

- mbledhjen e informacionit,
- krijimin e marrëdhënieve dhe raporteve,
- shfrytëzimin dhe
- 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.



URGENT



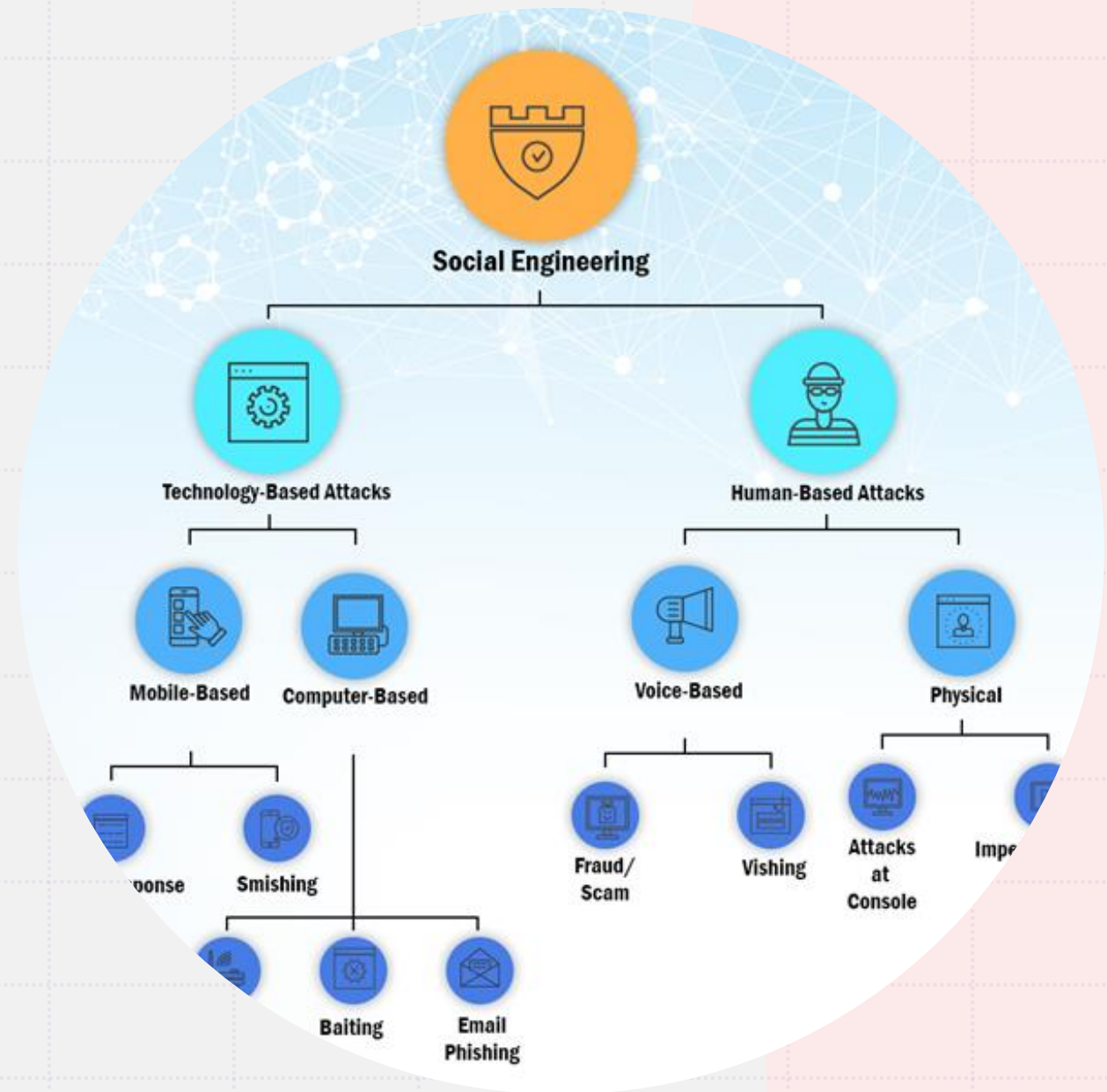


Qëllimet:

- 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 blikohet vetëm nga teknologjia.

"Njerëzit në përgjithësi janë të dobishëm, veçanërisht për dikë që është i mirë, i ditur ose këmbëngulës."

"Njerëzit në thelb duan të jenë të dobishëm dhe për këtë arsye mashtrohen lehtësisht."

"Në përgjithësi ne japin një nivel besimi për të shmangur konfliktin."

"E gjitha ka të bëjë me marrjen e aksesit në informacione që ne mendojmë se janë të padëmshme."

Tiparet e personalitetit

- Shpërndarja e përgjegjësisë
- Mundësi për miratim
- Marrëdhënie besimi
- Detyrë morale
- Faj
- Identifikim
- Dëshira për të qenë të dobishëm.
- Bashkëpunim



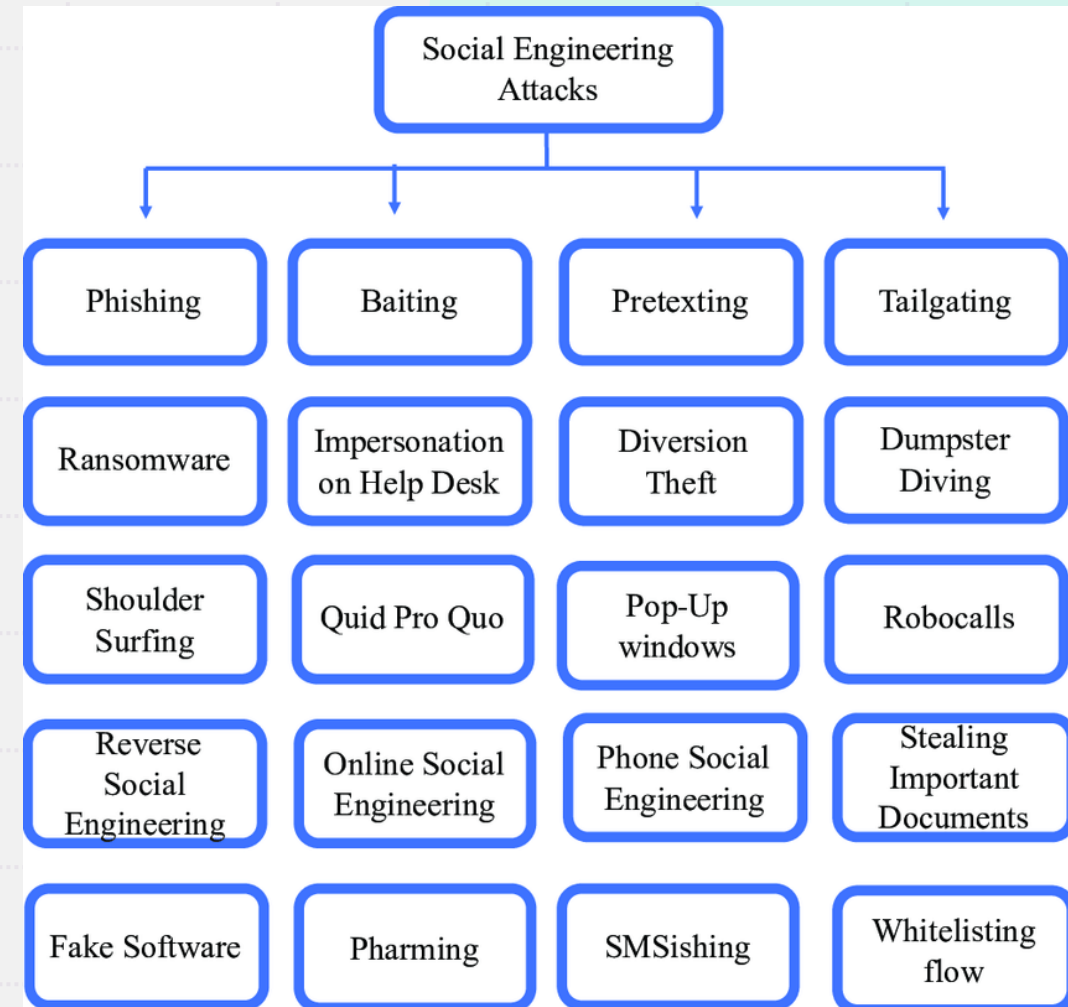
Sulmet tipike:

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



Metodat e 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

Email-et e phishing

- Një nga format më të zakonshme të inxhinierisë sociale janë emaillet e phishing.
- Ata shpesh duket se vijnë nga burime të besueshme, si bankat, faqet e mediave sociale, apo edhe punëdhënësi juaj.
- Zakonisht, emaillet përdorin taktika të frikësimit ose krijojnë një ndjenjë urgjence për t'ju detyruar të ndërmerri veprime urgjente.

FAKE

From: support@ricrosoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!



Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.liive.com/ResetPassword.aspx>

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity



Microsoft Account

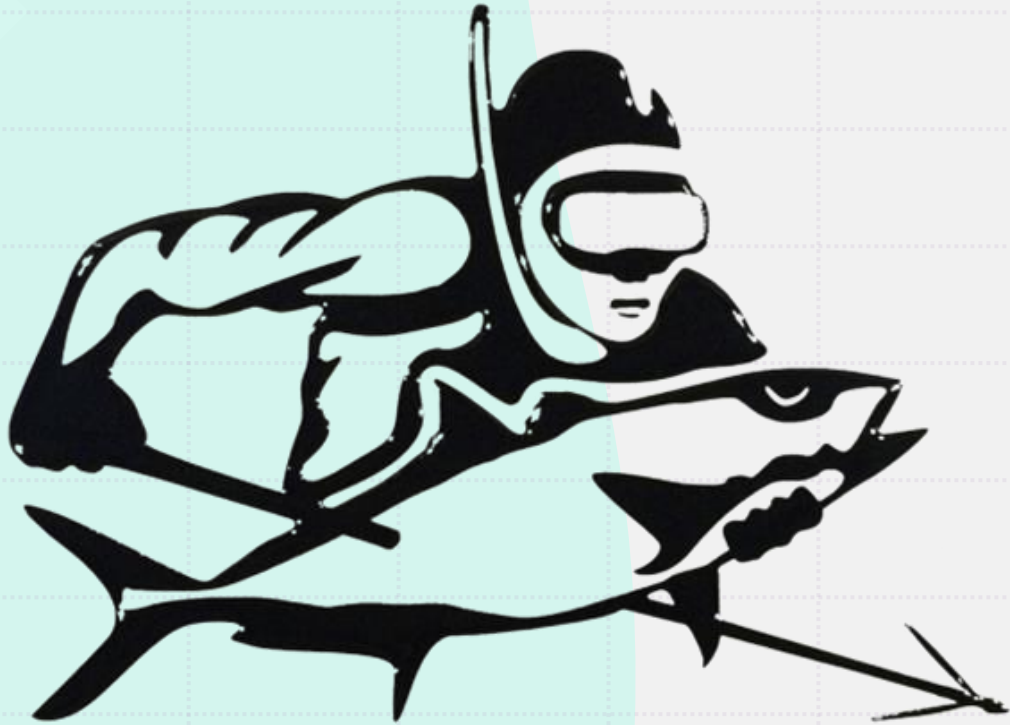
Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo*****@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

[Review recent activity](#)

Thanks,
The Microsoft Team



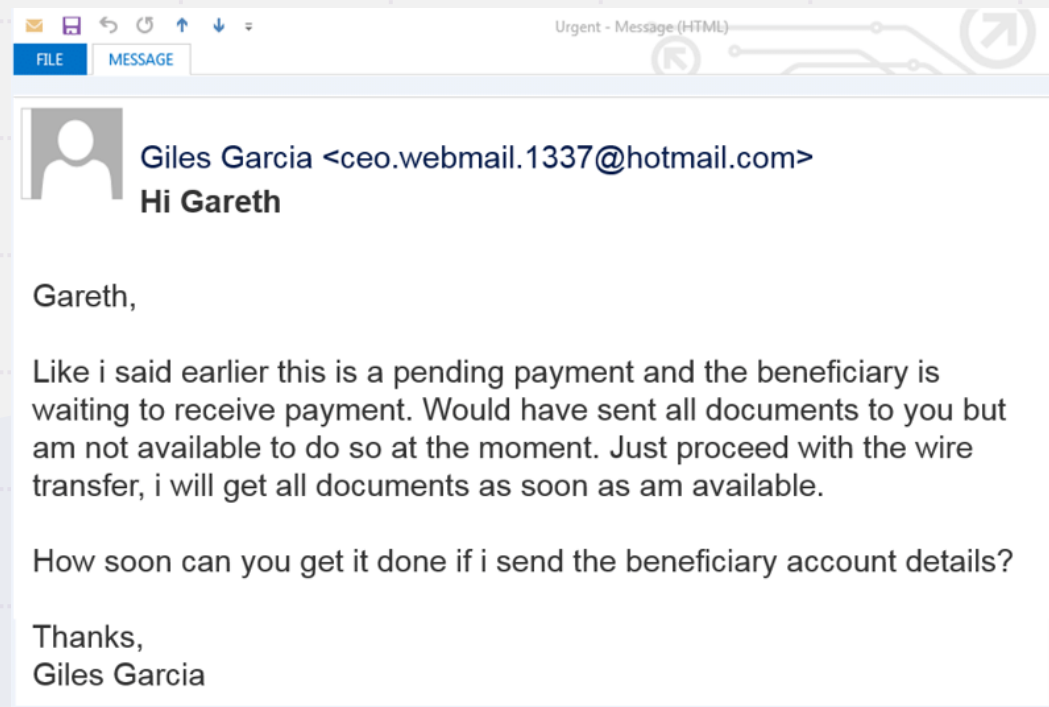
Spear Phishing

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

Whaling

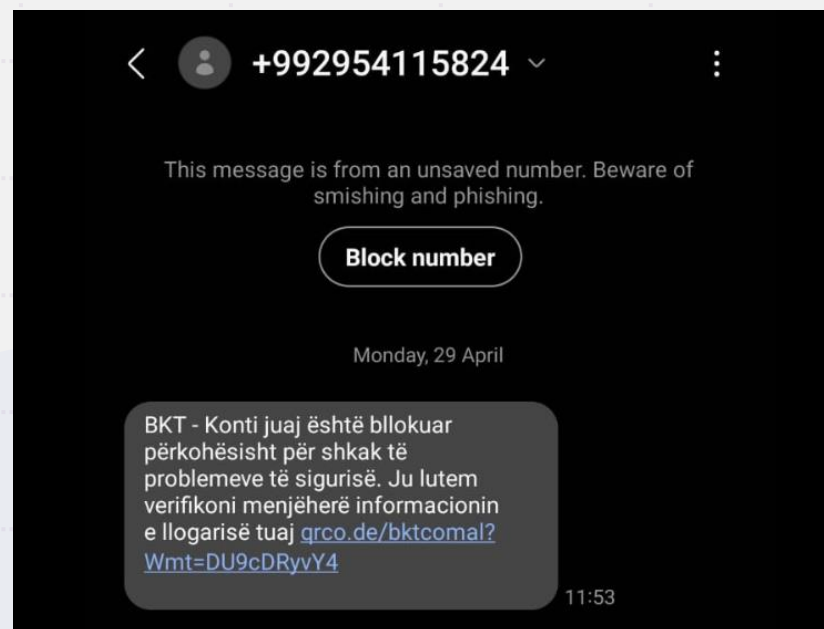
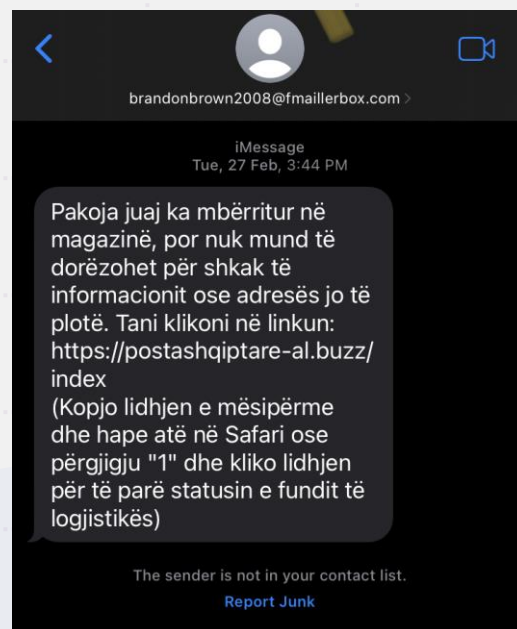


Një sulm i whaling, i njohur gjithashtu si gjueti për balena, është një lloj specifik sulmi phishing që synon punonjësit e profilit të lartë, si shefi ekzekutiv ose shefi financiar, për të vjedhur informacione të ndjeshme nga një kompani.

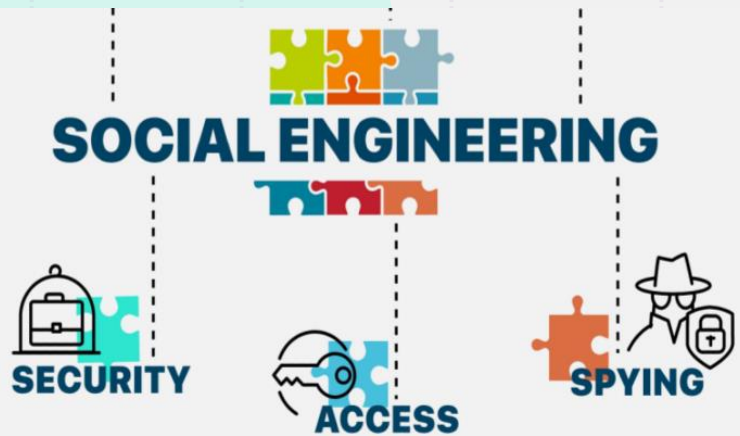


Smishing

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



Si të mos bini viktimë e një sulmi phishing:



- Mos e ndani fjalëkalimin tuaj me askënd
- Mos parapaguani në faqet e internetit të paverifikuara
- Mos shkruani një link në faqen e internetit në shfletuesin tuaj
- Mos shpërndani kodin CVV të kartës së pagesës dhe kodet nga SMS
- Mos vendosni pajisje USB të panjohura në kompjuterët tuaj
- Kontrolloni për kërkesa të dyshimta që kërkojnë veprim nga shefat dhe miqtë

Inxhinieria Sociale - Red Flags



DËRGUESI

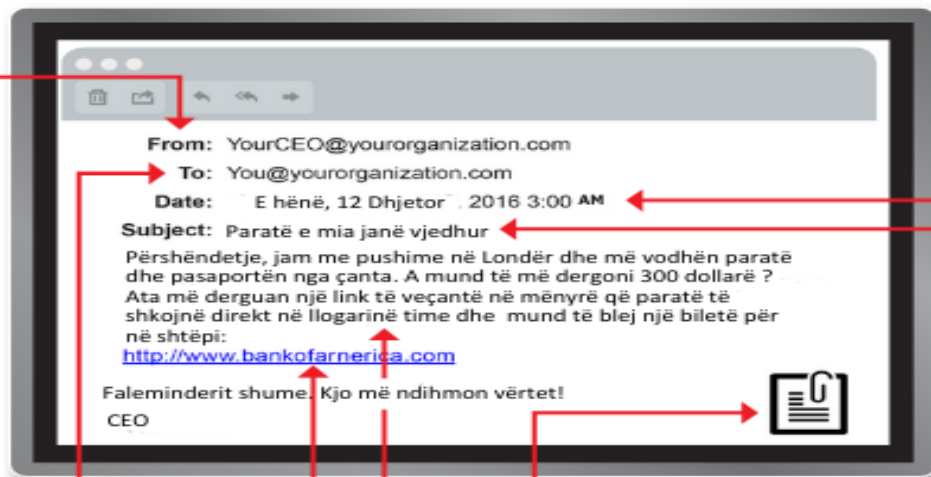
- Nuk e njihni adresën e emailit të dërguesit si dikë me të cilin **komunikoni zakonisht**.
- Ky email është nga dikush **jashtë organizatës dhe nuk është i lidhur me përgjegjësitë e punës**.
- Ky email është dërguar nga **dikush brenda organizatës** ose nga një klient, shitës ose partner dhe është **shumë i pazakontë**.
- A është adresa e emailit e dërguesit nga një **domain i dyshimtë?** (si për shembull: mikrosoft-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.

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.

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.bankofamerica.com - ku shkronja "m" është krijuar si bashkim i dy karaktere - "r" dhe "n".



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?**

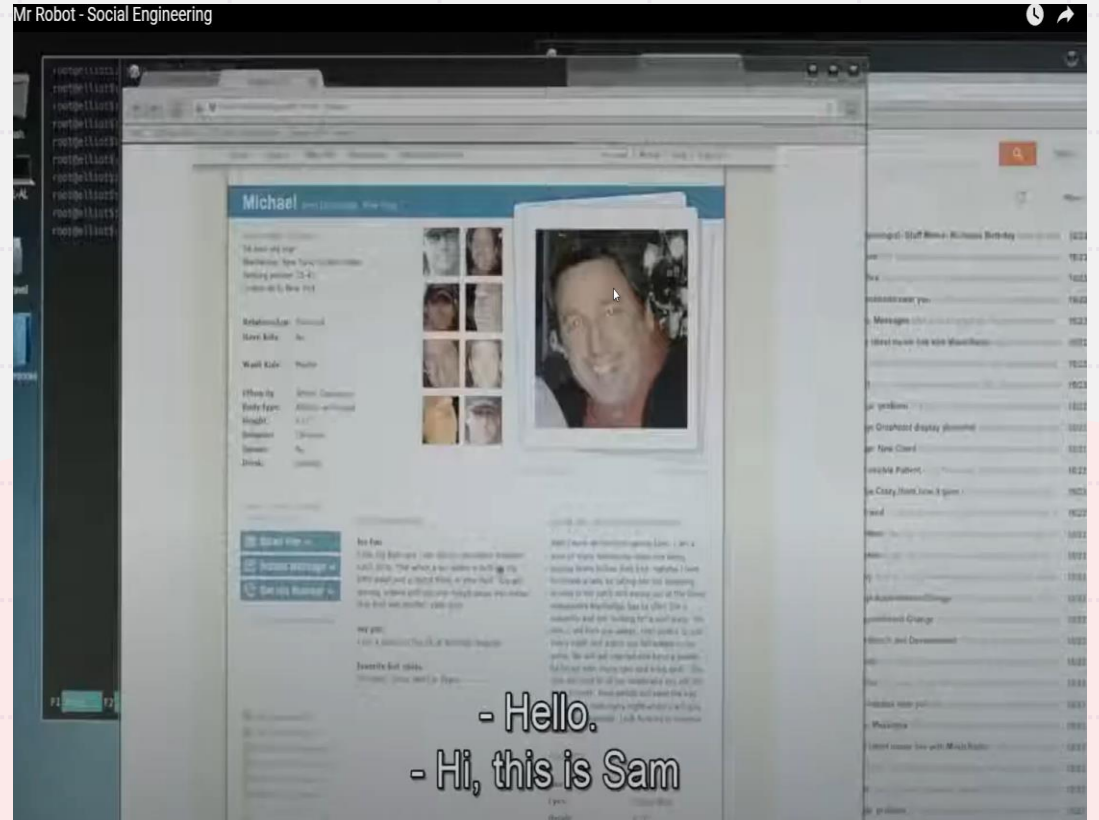
BASHKËNGJITJET

- 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**.

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 bashkëngjitur 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 komprometuese** ose **të sikletshme** të vetes suaj ose të dikujt që njihni?

Vishing - Zëri në anën tjetër



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/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.

Congratulations!
(1) \$1000 Amazon Gift Card is reserved for you!

Step 1: Click the "CONTINUE" button to claim your prize.

Step 2: Enter the correct information on the next page to claim your prize.

Important: Hurry, limited quantities only.

You only have **0 minutes 0 seconds to claim your prize!**



\$1000 Amazon Gift Card

CONTINUE

2 remaining!

Karrem fizik me një pajisje:

Eksperiment: Në një eksperiment të kontrolluar të kryer nga Universiteti i Miçiganit, Universiteti i 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 operativ ose 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

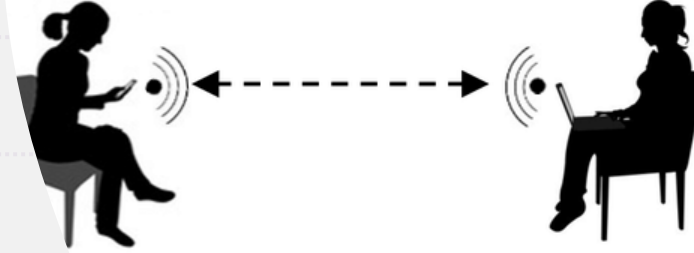
Diçka për diçka

Wireless interface/AP

Coffee Shop
SSID : FreeWiFi

Victim

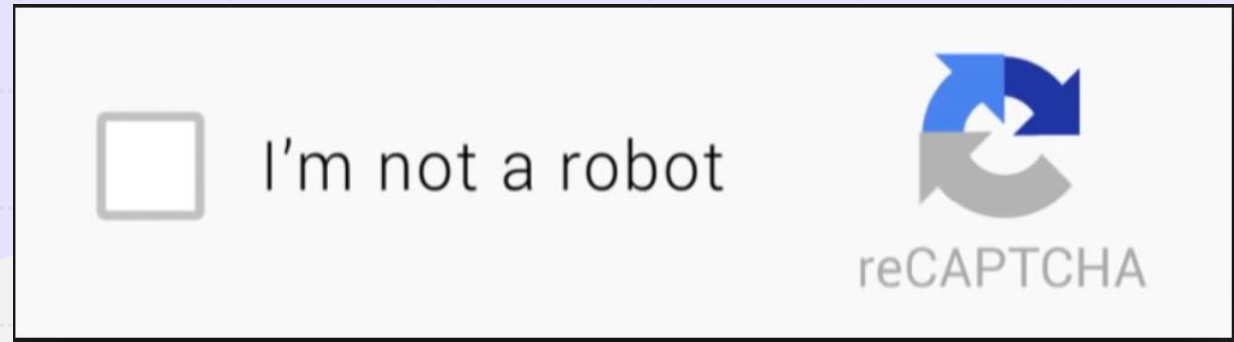
Attacker
SSID : FreeWiFi



Kuizet në Facebook

Dhurata të
kriptomonedhave

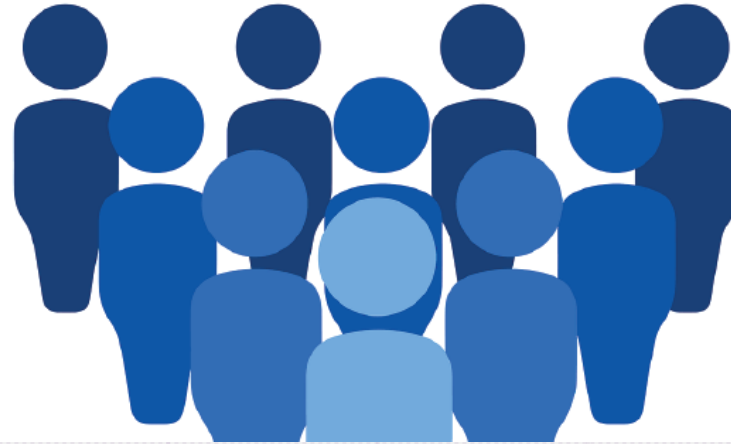




Kodet QR dhe testet CAPTCHA: Mashtrime të reja në një epokë dixhitale

Të skanosh apo të mos
skanosh?

LinkedIn



Rast Studimior: Imituesi i LinkedIn

Në këtë rast, një haker krijoi një profil të rremë LinkedIn, duke u paraqitur si një ekzekutiv i rangut të lartë në një institucion financiar prestigjioz. Sulmuesi kuroi me kujdes profilin e tyre, të kompletuar me një foto me pamje profesionale dhe një histori bindëse pune. Ai filloi të komunikojë me punonjësit në organizatën e synuar, duke ndërtuar ngadalë besimin.

Pasi sulmuesi kishte një rrjet të konsiderueshëm brenda organizatës, ai filloi të dërgonte mesazhe në dukje të padëmshme, duke kërkuar ndihmë për një projekt të supozuar urgjent. Këto mesazhe përmbanin bashkëngjitje me qëllim të keq që, kur hapeshin, lëshonin malware në kompjuterët e viktimave. Sulmuesi fitoi akses të paautorizuar në të dhënat e ndjeshme të kompanisë dhe bëri kërdi.

Si po shfrytëzohet Zoom për sulme phishing!

- Krijimi i një emaili phishing të Zoom
- Dërgimi i takimit të rremë të Zoom për viktimën
- Viktima klikon në linkun e phishing të takimit të Zoom.
- Kodi keqdashës ngarkohet në sistemin e viktimës.

Wed 6/24/2020 7:44 PM

Zoom Video Communications <help@raja.rr>

Emergency Zoom meeting

To: @uthscsa.edu

**Not Zoom;
E-mail originated
in Germany**

zoom
Video Conferencing

Dear @uthscsa.edu

You have received a video conference call invitation.

Review Invitation

Best
Team Zoom

**https://www.lightcityceramic.com/pagination/dj/
Opens malicious website**



Si të identifikoni një inxhinier social?

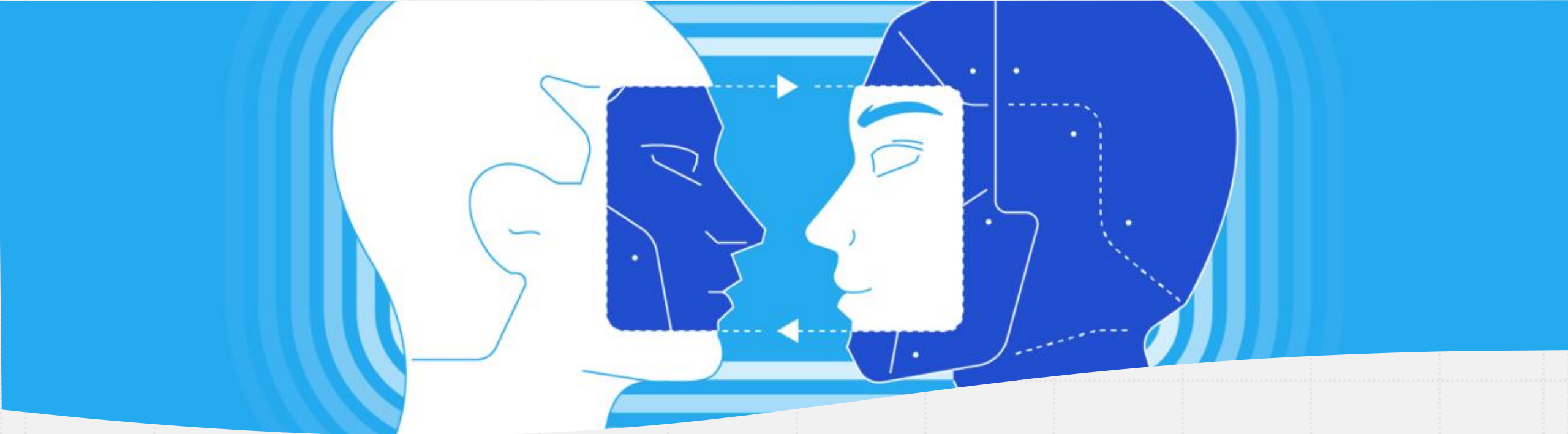
Nuk jep informacion kontakti

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
- Ndërgjegjësimi
- Patchime të përditësuara dhe azhurnim të Anti-Viruseve

KËSHILLA SI TË MBRONI VETEN TUAJ në nivel personal

- Injoroni kërkesat për informacione personale; verifikoni drejtpërdrejt me kompaninë.
- Vendosni një fjalëkalim unik të postës zanore në celular.
- Çaktivizo ndryshimet e kartës SIM, përcjelljen e thirrjeve, ziljen e njëkohshme me operatorin celular.
- Monitoroni historinë dhe ndryshimet e hyrjes në llogari.
- Mos ndani informacione personale në internet.
- Përdorni fjalëkalime unike, të forta; Mbi 14 karaktere.



KËSHILLA SI TË MBRONI VETEN TUAJ në nivel organizate

Etiketoni emailt 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 privileguara për anomali.

Ndaloni hyrjet anonime me VPN.

Edukoni stafin për inxhinierinë sociale, phishing.

Raportoni mesazhe të dyshimta.

Vërtetoni thirrjet nga shitësit e autorizuar me pakicë.



Paketa e Inxhinierisë Sociale

- Paketa e veglave të inxhinierisë sociale (SET) është një grup veglash me porosi të programuara në python, e cila fokusohet 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 shtojë dhe simulojë sulmet inxhinierike sociale dhe të lejojë testuesin të testojë në mënyrë efektive se si mund të ketë sukses një sulm i targetuar.

```
[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your t

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> █
```



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

Një vegël falas për të kontrolluar për shkelje të të dhënave.

email or phone (international format)

pwn

Faleminderit për vëmëndjen!

<https://cesk.gov.al/>

