TRAJNIM GJITHËPËRFSHIRËS MBI HIGJIENËN KIBERNETIKE, INTELIGJENCËN ME BURIM TË HAPUR (OSINT) DHE INXHINIERINË SOCIALE.

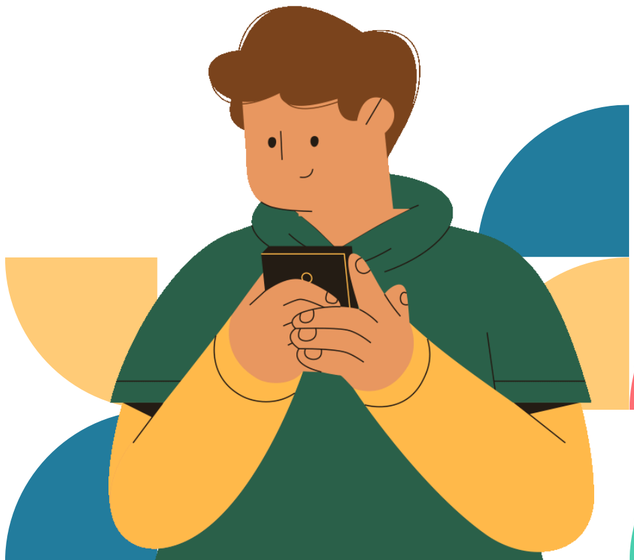
HYRJE NË HIGJIENËN KIBERNETIKE

- Rëndësia e higjienës kibernetike
- Panorama aktuale e kërcënimeve kibernetike
- Parimet bazë të higjienës kibernetike

RËNDËSIA E HIGJIENËS KIBERNETIKE

Në jetën e përditshme ne mbështetemi te kompjuterët dhe interneti për:

- **Komunikim** (email, smartphone, tablet)
- **Argëtim** (lojëra, video interaktive, media sociale, aplikacione)
- **Transport** (sistemet e navigimit)
- **Blerje** (blerje në internet, kartë krediti)
- **Mjekësi** (pajisje mjekësore, të dhëna mjekësore) etj...



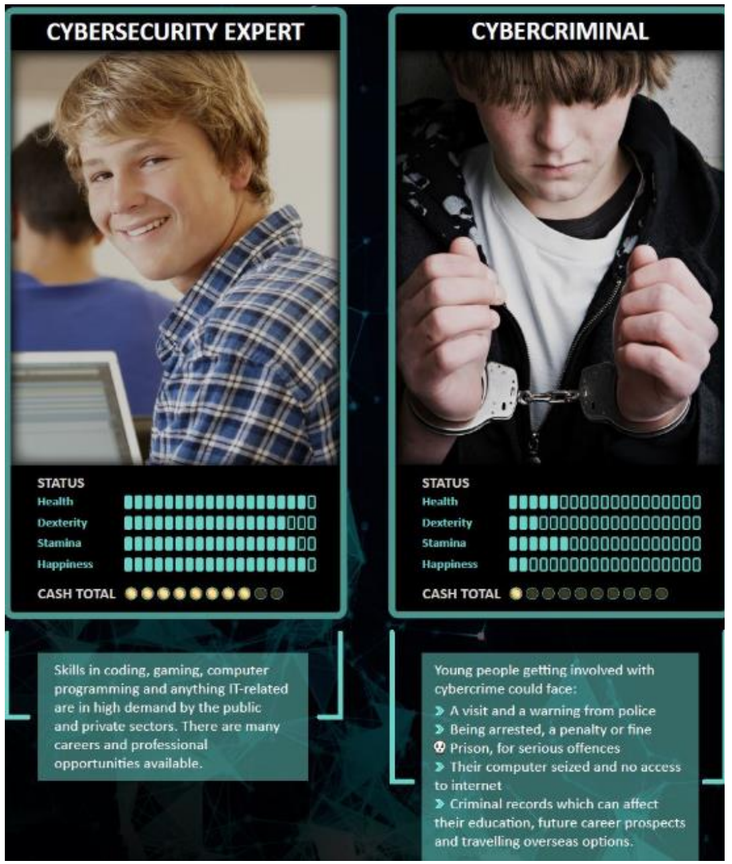
ÇFARË ËSHTË SIGURIA KIBERNETIKE

Siguria kibernetike është **arti** i mbrojtjes së **rrjeteve**, **pajisjeve** dhe **të dhënave** nga aksesi i paautorizuar ose përdorimi kriminal!

Është gjithashtu **praktikë** e sigurimit të **konfidencialitetit**, **integritetit** dhe **disponueshmërisë** së informacionit.

DILEMË

Siguria Kibernetike vs Krimi Kibernetik



Siguria Kibernetike
Gjendje
[**e Dëshiruar**]

Gjëndja e të qënit i/e mbrojtur kundër përdorimit kriminal ose të paautorizuar të të dhënave elektronike, ose masat e marra për të arritur këtë.

Krimi Kibernetik
Aktivitet
[**i Padëshiruar**]

Çdo sjellje e paligjshme e drejtuar përmes operacioneve elektronike që synon të cënojë sigurinë e sistemve kompjuterike dhe të dhënave të përpunuara prej tyre.

MOTIVET DHE SOFISTIKIMI PO EVOLUOJNË ME SHPEJTËSI!

Konkurrentë dhe Aktivistë

Aurora

Grupi Aurora, një grup hakerash i dyshuar i sponsorizuar nga shteti kinez, synoi kompanitë e teknologjisë amerikane që nga viti 2009 e tutje, duke vjedhur pronën intelektuale dhe të dhëna të ndjeshme. Sulmet e tyre të sofistikuara nxorën në pah cenueshmërinë e korporatave të mëdha ndaj spiunazhit kibernetik dhe nevojën për masa të forta të sigurisë kibernetike.

Punonjës të brendshëm dhe Script-kiddies

Code Red

Code Red ishte një krimb i përhapur që shfrytëzoi një dobësi në serverët e uebit të Microsoft IIS në 2001. Ai shkaktoi ndërprerje të konsiderueshme duke ngarkuar sistemet e infektuara me sulme të mohimit të shërbimit (DoS) dhe duke ndërprerë shërbimin për faqet e internetit. Ky incident nënvizoi cenueshmërinë e sistemeve të lidhura me internetin dhe nevojën për masa proaktive sigurie.

Siguria Kombëtare

Spiunazh, Aktivizëm

Fitim Monetar

Hakmarrje, Kuriozitet

Aktorë Shtetërorë

Stuxnet

Stuxnet, një pjesë e sofistikuar e malware, u zbulua në vitin 2010. Ai ishte projektuar për të synuar objektet bërthamore iraniane, veçanërisht centrifugat e përdorura në pasurimin e uraniumit. Stuxnet besohej të ishte një operacion i përbashkët nga Shtetet e Bashkuara dhe Izraeli, duke e bërë atë një nga rastet e para të njohura të luftës kibernetike të sponsorizuar nga shteti.

Krim i organizuar

Zeus

Zeus Group ishte një organizatë famëkeqe e krimit kibernetik që përdorte malware të sofistikuar për të vjedhur informacione financiare nga klientët e sektorit bankar online në mbarë botën, duke shkaktuar humbje të konsiderueshme si për individët ashtu edhe për institucionet.

MUNGESA E KUFIJËVE

Krimi kibernetik nuk njeh kufij, duke e bërë atë një sfidë globale që kërkon bashkëpunim ndërkombëtar. Natyra dixhitale e sulmeve kibernetike i lejon kriminelët të veprojnë nga kudo në botë, duke e bërë të vështirë për vendet individuale që ta trajtojnë këtë çështje vetëm.

Për të luftuar në mënyrë efektive krimin kibernetik, qeveritë, agjencitë e zbatimit të ligjit dhe organizatat e sektorit privat duhet të punojnë së bashku për të shkëmbyer informacione, për të zhvilluar praktikat më të mira dhe për të zbatuar ligjet ndërkombëtare.

PANORAMA AKTUALE E RREZIQEVE KIBERNETIKE

Le të flasim për disa nga termat e rëndësishëm për t'u mbajtur mend që do t'ju ndihmojnë të dalloni rreziqet e një sulmi kibernetik.

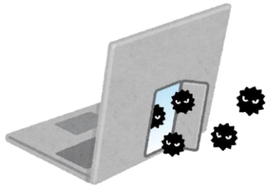
Haker apo Sulmues

Këta janë njerëzit që shfrytëzojnë dobësitë në softuer dhe sisteme kompjuterike për përfitimin e tyre!

Malware/Program Keqdashës

Malware (i quajtur edhe program me qëllim të keq) janë skedarë ose programe të padëshiruara që mund të shkaktojnë dëme në një kompjuter ose kompromentojnë të dhënat e ruajtura në një kompjuter.

Vulnerabilitete/Dobësitë



Dobësitë janë të meta në softuer, firmware ose harduer që mund të shfrytëzohen nga një sulmues për të kryer veprime të paautorizuara në një sistem.

KËRCËNIMET E ZAKONSHME KIBERNETIKE

MALWARE

1

Virusët, Krimbat, Trojanët

MALWARE: Softuer i krijiuar për të prishur, dëmtuar ose për të fituar akses të pa-autorizuar

PHISHING

2

Email-e dhe faqe Interneti mashtruese

PHISHING: Përpjekje mashtruese për të marrë informacion të ndjeshëm

RANSOMWARE

3

Enkriptimi i të dhënave për shpërblim

RANSOMWARE: Një lloj malware që bllokon skedarët tuaj deri sa të paguhet një shpërblim

KËRCËNIMET E ZAKONSHME KIBERNETIKE

INFESKSIONET MALWARE

- Viruse, krimba dhe Trojanë
- Ransomware që enkripton të dhënat për shpërblim
- Spyware që ndjek aktivitete e përdoruesit

SULMET PHISHING

- Email-e dhe mesazhe mashtruese
- Faqe Interneti të rreme që imitojnë ato legjitime
- Mashtrojnë përdoruesit për të zbuluar informacion të ndjeshëm

SULMET RANSOMWARE

- Enkriptimi i të dhënave të përoduresit
- Kërkesa shpërblimi për dekriptim
- Shkaktim i humbjes së të dhënave dhe dëme financiare

SULMET E MOHIMIT TË SHËRBIMIT (DoS)

- Mbingarkimi i sistemeve për të shkaktuar ndërprerje
- DoS i Shpërndarë (DDoS) duke përdorur sisteme të shumta
- Ndërprerja e shërbimeve dhe aksesit në shërbime

KËRCËNIMET E ZAKONSHME KIBERNETIKE

SULMET "NJERIU NË MES" (MITM)

- Përgjimi i komunikimeve
- Dëgjimi i fshehtë i transmetimit të të dhënave
- Vendosja e përmbajtjes së dëmshme në komunikim

SULMET ME SQL INJECTION

- Shfrytëzimi i dobësive në aplikacionet Web
- Vendosja e kodit të dëmshëm SQL
- Fitim i aksesit të paautorizuar në bazat e të dhënave

SULMET E INXHINIERISË SOCIALE

- Manipulimi i individëve për të zbuluar informacion konfidencial
- Përdorimi i manipulimit psikologjik
- Paraqitja si persona ose entitete të besueshëm

SHFRYTËZIMET ZERO-DAY EXPLOITS

- Shfrytëzimi i dobësive të panjohura
- Shfrytëzimi i të metave të softuerit përpara se të jenë të disponueshme arnimet
- Shkaktimi i dëmeve të mëdha përpara zbulimit

KLASIFIKIMI I MALWARE-VE

VIRUSET

Viruset janë një lloj i përgjithshëm i programeve keqdashëse që janë të aftë të infektojnë kompjuterët dhe zakonisht përhapen përmes ndërveprimeve njerëzore ose duke shfrytëzuar dobësië e sistemit.

Viruset **nuk krijohen vetvetiu**, por programohen nga specialistët e kompjuterëve për të kryer funksione të ndryshme keqdashëse.

KLASIFIKIMI I MALWARE-VE

KRIMBAT

Krimbat janë një lloj virusi që **vetë-përhapen** nga një kompjuter tek tjetri.

Funksionaliteti i tyre është të përdorin të gjitha burimet e kompjuterit tuaj, gjë që mund të shkaktojë që kompjuteri juaj të mos përgjigjet komandave.

KLASIFIKIMI I MALWARE-VE

DALLIMI
VIRUS vs KRIMB

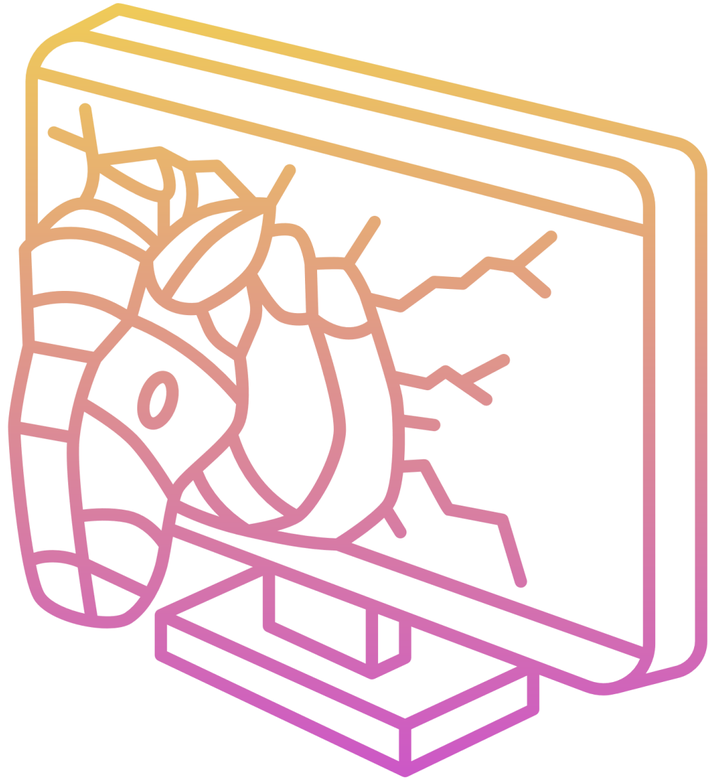
Një krimb **mund të vetë riprodhohet** dhe të përhapet nga një kompjuter në tjetrin.

Nga ana tjetër, **një virus nuk mund të riprodhohet vetë** dhe ka nevojë të dërgohet nga një përdorues ose softuer për të udhëtuar midis dy kompjuterave të ndryshëm.

KLASIFIKIMI I MALWARE-VE

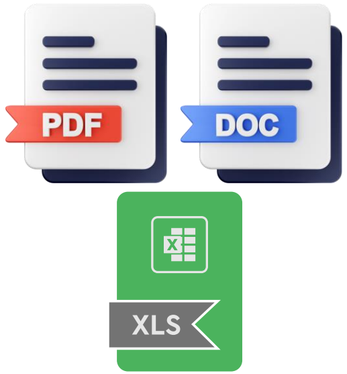
TROJANËT

Trojanët janë programe kompjuterike që fshehin një virus ose një program potencialisht të dëmshëm. **Nuk është e pazakontë që softuerët falas të përmbajnë një Trojan**, duke bërë që përdoruesi të mendojë se po përdor një softuer të ligjshëm, ndërsa programi në fakt kryen veprime të dëmshmë në kompjuterin tuaj.



KLASIFIKIMI I MALWARE-VE

SKEDARËT E TË DHËNAVE TË DËMSHME (MALICIOUS)



Skedarët e të dhënave të dëmshme janë skedarë apo dokumenta **jo-ekzekutues - si një dokument Microsoft Word, një PDF Adobe, një skedar ZIP** ose një skedar imazhi që shfrytëzon dobësitë në programin e softuerit të përdorur për ta hapur atë.

Sulmuesit shpesh përdorin skedarë të dhënash të dëmshme për të instaluar malware në sistemin e viktimës, duke shpërndarë skedarët përmes email-it, rrjeteve sociale dhe faqeve të internetit.

SHEMBUJ NGA BOTA REALE

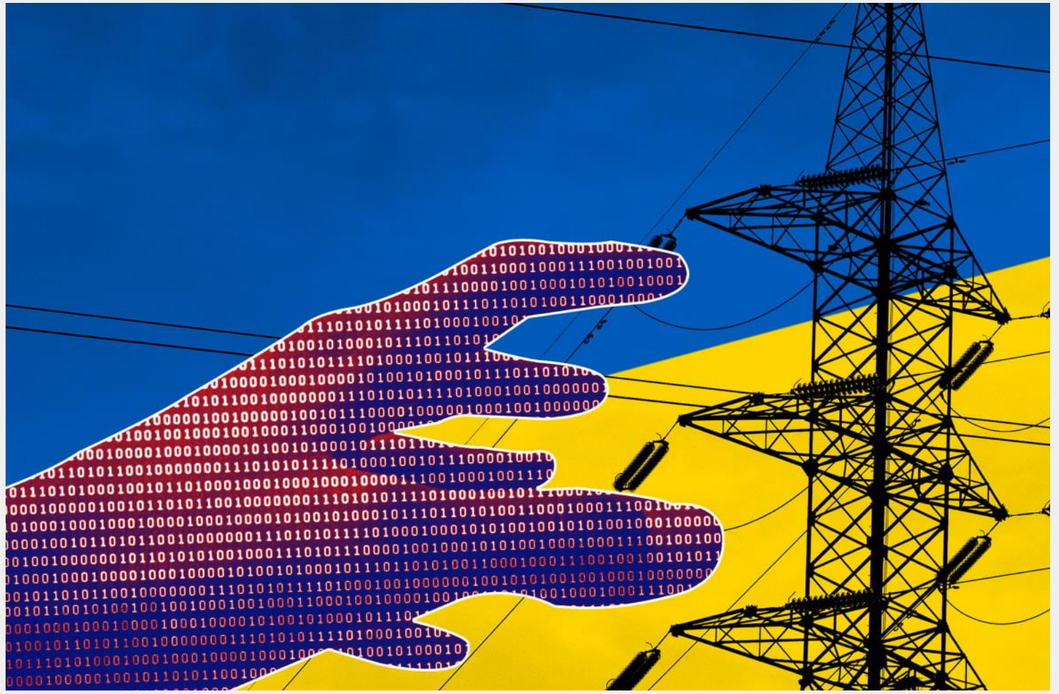
Sulmet kibernetike vijnë në forma të ndryshme, secila me karakteristikat dhe objektivat e veta unike. Këto sulme mund të kenë pasoja shkatërruese për individët, bizneset dhe infrastrukturën kritike.

RRJETI ENERGJETIK I UKRAINËS, 2016

Kërcënim: Ndërprerje të energjisë elektrike, mungesë ngrohje
Autori i dyshuar: grupi rus i hakerëve "Sandworm"
Lloji i sulmit: DDoS, Spear phishing

Në mes të dimrit, gjysma e popullsisë së një rajoni në Ukrainë (700,000 njerëz) u gjend pa energji elektrike. Arsyeja ishte për shkak të një sulmi malware në impiantin e energjisë të vendit pas një breshëri sulmesh DDoS, spear phishing dhe rrëmbimit të Border Gateway Protocol.

Kompanitë, si dhe individët privatë, morën peshën kryesore të sulmit duke pësuar ndërprerje në biznes dhe në jetën e tyre të përditshme.



SEKTORI I FURNIZIMIT ME UJË TË IZRAELIT, 2020

Kërcënim: Sistemet e kompromentuara të ujit, helmimi me klor
Autori i dyshuar: I panjohur
Lloji i sulmit: Pajisje e lidhur me rrjetin e panjohur

Gjatë pikut të Covid-19 dhe një vale të pandërprerë të nxehtit, sistemet izraelite të ujit duruan sulme të shumta kibernetike të krijuara për të kompromentuar sistemet e kontrollit për stacionet e pompimit, impiantet e ujërave të zeza dhe pompat bujqësore.

Megjithëse sulmet ishin të pasuksesshme, ato synonin të nxisnin klorin dhe kimikatet e tjera në nivele të dëmshme në ujin publik, duke ndërprerë furnizimin në një kohë kritike për Izraelin. Sikur sulmi të ishte i suksesshëm, civilët do të mbingarkonin më tej spitalet, fermerët do të shkatërronin pa dashje të korrat e tyre dhe implikimet e mëtejshme do të shkatërronin vendin gjatë një pandemie.

WANNA CRY RANSOMWARE 2017

Kërcënim: Skedarë të koduar, humbje të të dhënave, ndërprerje biznesi, humbje financiare
Autori i dyshuar: Grupi Lazarus, një grup hakerash i sponsorizuar nga shteti i Koresë së Veriut
Lloji i sulmit: Ransomware, krimb (vetëshpërndahet)

Ransomware WannaCry ishte një sulm global shkatërrues që shfrytëzoi një dobësi në sistemet Microsoft Windows në 2017 duke infektuar 200,000 kompjutera. Malware kodonte skedarët në pajisjet e infektuara dhe kërkonte një pagesë shpërblimi në bitcoin për deshifrim. Sulmi shkaktoi përçarje të gjerë në bizneset, spitalet dhe organizatat e tjera në mbarë botën, duke theksuar kërcënimin serioz që vjen nga ransomware.

SULMET E AKTORËVE SHTETËROR (APT) DREJT SHQIPËRISË

How Albania Became a Target for Cyberattacks

A massive hack led to the expulsion of Iranian diplomats—but Tehran may have had help fr
Moscow.

Iran-linked hackers claim attack on Albania's Institute of Statistics

An Iran-linked hacking group with a history of targeting Albanian state agencies
businesses said on Thursday that it was behind an attack on the country's Institu
Statistics (INSTAT), which is responsible for census information and other official

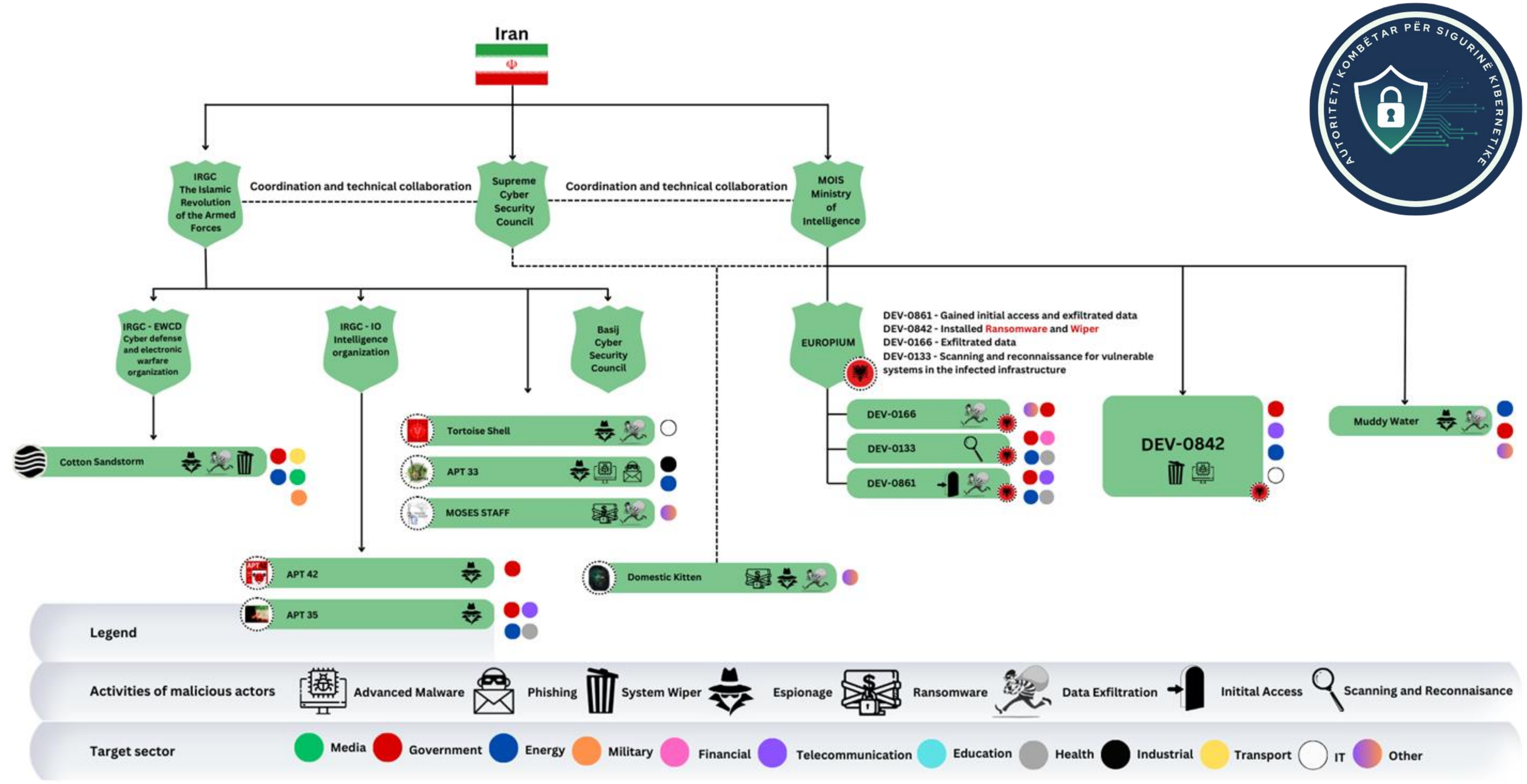
Due to the "sophisticated" cyber incident that affected INSTAT's official website
service, the agency announced that it would postpone the release of official stat
further notice.

Albania cuts diplomatic ties with Iran over cyberattack

Tirana expels the Iranian embassy staff over a cyberattack allegedly carried out on the government websites in July.

Wiper malware found in analysis of Iran-linked attacks on Albanian institutions

During the wave of attacks on Albanian organizations earlier in December, Iran-linked


Iran
IRGC
The Islamic Revolution of the Armed Forces
Coordination and technical collaboration
Supreme Cyber Security Council
Coordination and technical collaboration
MOIS
Ministry of Intelligence
IRGC - EWCD
Cyber defense and electronic warfare organization
IRGC - IO
Intelligence organization
Basij
Cyber Security Council
EUROPIUM
DEV-0861 - Gained initial access and exfiltrated data
DEV-0842 - Installed Ransomware and Wiper
DEV-0166 - Exfiltrated data
DEV-0133 - Scanning and reconnaissance for vulnerable systems in the infected infrastructure
Cotton Sandstorm
Tortoise Shell
APT 33
MOSES STAFF
DEV-0166
DEV-0133
DEV-0861
DEV-0842
Muddy Water
APT 42
APT 35
Domestic Kitten
Legend
Activities of malicious actors
Advanced Malware
Phishing
System Wiper
Espionage
Ransomware
Data Exfiltration
Initital Access
Scanning and Reconnaisance
Target sector
Media
Government
Energy
Military
Financial
Telecommunication
Education
Health
Industrial
Transport
IT
Other

CEO I WPP - BIEN VIKTIME E NJË MASHTRIMI ME DEEP FAKE

- Mark Read, CEO i Wire and Plastic Products (WPP), ishte pre e një mashtrimi deepfake.
- Mashtruesit klonuan zërin e tij dhe krujuan një llogari të rreme në Whatsapp duke përdorur foton e tij.
- Ata u përpoqën të kërkonin para dhe detaje personale nga udhëheqësit e WPP.

SI U EKZEKUTUA MASHTRIMI?

- Mashtruesit përdorën një foto të Mark Read për një profil Whatsapp për tu dukur të besueshëm
- U organizua një takim në Microsoft Teams me ekzekutivët e WPP duke përdorur llogarinë e rreme.
- Gjatë takimit, u përdor një video dhe zë i klonuar i Mark Read
- Funksioni i bisedës u përdor gjithashtu për të imituar Read për të kërkuar informacion

REAGIMI DHE REZULTATI

- Përpjekja e mashtrimit u identifikua dhe u parandalua nga punonjësit vigjilentë të WPP.
- Mark Read theksoi nevojën për vigjilencë kundër sulmeve të sofistikuara kibernetike.
- WPP konfirmoi përpjekjen e pasuksesshme

KONTEKSTI DHE IMPLIKIMET E GJËRA

- Ky incident ve në pah sofistikimin në rritje të sulmeve kibernetike.
- Teknologjia DeepFake po bëhet një mjet i rëndësishëm në mashtrimet kibernetike.
- Kapitali tregëtar i WPP është rreth 11.3 Miliardë Dollarë, duke treguar peshën e madhe të përfshirë.

SHENJAT PARALAJMËRUESE DHE MASAT PARANDALUESE

- Kushtojini vëmëndje kërkesave të pazakonta si pasaporta, transferta parash, ose transaksione sekrete.
- Jini skeptik ndaj komunikimeve që duken të pazakonta ose të paverifikuara.
- Mark Read: "Vetëm sepse llogaria ka foton time nuk do të thotë që jam unë"

PËRFUNDIMI DHE PRESPEKTIVAT E ARDHSHME

- Nevoja për masa të avancuara të sigurisë kibernetike është më kritike se kurrë.
- Kompanitë duhet të trajnojnë punonjësit për të njohur dhe raportuar kërcënimet e mundshme kibernetike.
- Panorama në Zhvillim i AI dhe DeepFakes kërkon monitorim dhe përshtatje të vazhdueshme.

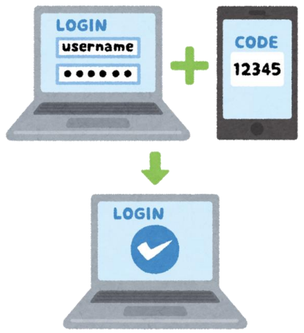
MEDIAT THEKSOJNË VETËM MAJËN E AJSBERGUT

Sulmet Kibernetike të përmendura në shtyp

Sulmet Kibernetike të zbuluara, por të papërmendura

Sulmet Kibernetike të pazbuluara

FAKTORI NJERI



Problemi më i madh në Sigurinë Kibernetike nuk është Firewall-i apo Antivirusi.

Është faktori njerëzor. Ne jemi hallka më e dobët!

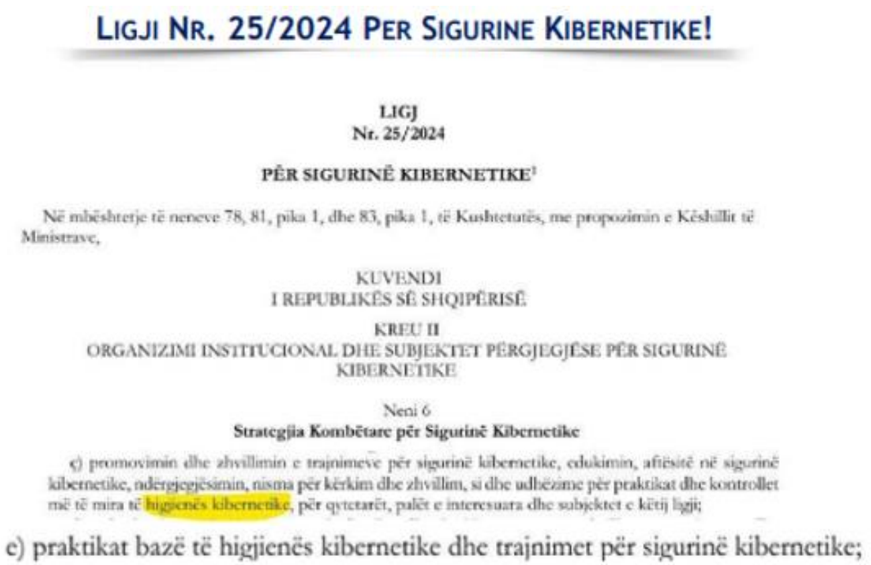
Ne marrim vendime të gabuara, shpesh për shkak të kufizimeve të kohës ose mungesës së kuptimit. Dhe ndonjëherë, kemi një mendësi vetë-shkatëruese që na vë në rrezik ne dhe të tjerët.

DILEMA

Po sikur t'i trajnojmë dhe ata largohen?

Po sikur të mos i trajnojmë dhe ata qëndrojnë?

LIGJI NR. 25/2024 PËR SIGURINË KIBERNETIKE!



LIGJI NR. 25/2024 PER SIGURINE KIBERNETIKE!

LIGJ
Nr. 25/2024

PËR SIGURINË KIBERNETIKE[1]

Në mbështetje të neneve 78, 81, pika 1, dhe 83, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave,

KUVENDI
I REPUBLIKËS SË SHQIPËRISË

KREU II
ORGANIZIMI INSTITUCIONAL DHE SUBJEKTET PËRGJEGJËSE PËR SIGURINË KIBERNETIKE

Neni 6
Strategjia Kombëtare për Sigurinë Kibernetike

ç) promovimin dhe zhvillimin e trajnimeve për sigurinë kibernetike, edukimin, aftësitë në sigurinë kibernetike, ndërgjegjësimin, nisma për kërkim dhe zhvillim, si dhe udhëzime për praktikat dhe kontrollet më të mira të higjienës kibernetike, për qytetarët, palët e interesuara dhe subjektet e këtij ligji;

e) praktikat bazë të higjienës kibernetike dhe trajnimet për sigurinë kibernetike;

Neni 6
Strategjia Kombëtare për Sigurinë Kibernetike

Synon promovimin dhe zhvillimin e trajnimeve për sigurinë kibernetike, edukimin, aftësitë në sigurinë kibernetike, ndërgjegjësimin, nisma për kërkim dhe zhvillim, si dhe udhëzime për praktikat dhe kontrollet më të mira të higjienës kibernetike, për qytetarët, palët e interesuara dhe subjektet e këtij ligji;

DIREKTIVA NIS 2

NIS 2 synon të rrisë sigurinë kibernetike të rrjeteve dhe sistemeve të informacionit në të gjithë Bashkimin Evropian. Duke u kërkuar operatorëve të shërbimeve kritike dhe të rëndësishme të zbatojnë masat e duhura të sigurisë dhe të raportojnë incidentet tek autoritetet, NIS 2 kërkon të reduktojë rrezikun e sulmeve kibernetike dhe të përmirësojë qëndrueshmërinë e përgjithshme të infrastrukturës kritike. Direktiva synon gjithashtu të nxisë bashkëpunimin midis shteteve anëtare dhe të rrisë efektivitetin e përpjekjeve të reagimit ndaj sigurisë kibernetike.

PARIMET BAZË TË HIGJIENËS KIBERNETIKE

Higjiena Kibernetike i referohet praktikave dhe hapave që përdoruesit dhe organizatat ndërmarrin për të ruajtur qëndrueshmërinë dhe sigurinë e sistemeve të tyre. Kjo përfshin mirëmbajtjen e rregullt, përditësimet e softuerit dhe adoptimin e masave të sigurisë.

Duke praktikuar higjienë të mirë kibernetike, mund të mbroni sistemet tuaja nga kërcënime të ndryshme kibernetike. Kjo është thelbësore sepse ndihmon në sigurinë që informacioni i ndjeshëm të ruhet i sigurt dhe që sistemet të funksionojnë pa ndërprerje.

HIGJIENA KIBERNETIKE MBROJTJA E TË DHËNAVE TË NDJESHME QEVERITARE

Praktikat e mira të higjenës kibernetike gjithashtu ndihmojnë në ndërtimin e një kulture të ndërgjegjësimit për sigurinë brenda oganizatës ose institucionit tuaj.

Institucionet qeveritare në Shqipëri trajtojnë një sasi të madhe informacioni konfidencial dhe një shkelje e sigurisë mund të ketë pasoja të rënda.

REPUBLIKA E SHQIPËRISË

SI TË MBROHENI NGA MALWARE?

1. Instaloni dhe mirëmbani softuerin antivirus
2. Kini kujdes me linqet dhe bashkëngjitjet
3. Bllokoni reklamat pop-up
4. Përdorni një llogari me leje të kufizuara
5. Ç'aktivizoni funksionet AutoRun dhe AutoPlay të mediave të jashtme
6. Ndryshoni fjalëkalimet tuaja
7. Mbani të përditësuar sistemin operativ
8. Përdorni një firewall për të bllokuar aksesin e paautorizuar

HAPA TË TJERË PËR TU MBROJTUR NGA MALWARE?

1. Mbani të përditësuar softueret tuaja
2. Krijoni kopje rezervë të të dhënave
3. Instaloni ose ekzekutoni një firewall
4. Përdorni mjete anti-spyware
5. Monitoroni llogaritë
6. Shmangni përdorimin e Wi-Fi publik
7. Edukohuni për taktikat phishing
8. Rishikoni dhe rregulloni vazhdimisht konfigurimet e privatësisë në rrjetet sociale

ÇFARË DUHET TË DINI RRETH PROGRAMEVE ANTIVIRUS

Programet Antivirus skanojnë skedarët dhe memorien e kompjuterit për modele që tregojnë praninë e mundshme të kodit të dëmshëm. Ju mund të kryeni skanime antivirus automatikisht ose manualisht.

SKANIMET AUTOMATIKE

Shumica e programeve antivirus mund të skanojë automatikisht skedarë ose direktori të veçanta.

SKANIMET MANUALE

Nëse programi juaj antivirus nuk skanon automatikisht skedarët e rinj, duhet t'i skanoni manualisht ato dhe pajisjet si USB që merrni nga burime të jashtme përpara se t'i hapni.

SI TË RIMARRNI VETEN NËSE BËHENI VIKTIMË E MALWARE

Përdorimi i programeve antivirus është mënyra më e mirë për të mbrojtur kompjuterin tuaj nga kodi i dëmshëm. Nëse mendoni se kompjuteri juaj është infektuar startoni programin tuaj antivirus.

Idealisht, programi juaj antivirus do të identifikojë çdo kod të dëmshëm në kompjuterin tuaj dhe do ti karantinojë ato, në mënyrë që të mos ndikojnë më në sistemin tuaj.

MBAJENI SOFTUERIN TË PËRDITËSUAR

Instaloni patch-et e softuerit në mënyrë që sulmuesit të mos përfitojnë nga problemet ose dobësitë e njohura. Shumë sisteme operative ofrojnë përditësime automatike. Nëse kjo mundësi është e disponueshme, duhet ta aktivizoni.

PËRDORNI FJALËKALIME TË FORTA

Zgjidhi fjalëkalime që do të jenë të vështira për t'u marrë me mend nga sulmuesit dhe përdorni fjalëkalime të ndryshme për programe dhe pajisje të ndryshme.

Është më mirë të përdorni fraza të gjata, të forta ose fjalëkalime që përbëhen të paktën nga 16 karakterë.

TEKNIKA PËR TË ZHVILLUAR FJALËKALIME UNIKE PËR ÇDO LLOGARI TUAJËN

Përdorni fjalëkalime të ndryshme në sisteme dhe llogari të ndryshme.

- Zhvilloni mnemonika për të mbajtur mend fjalëkalime komplekse
- Përdorni fjalëkalimin ose frazën më të gjatë të lejuar nga çdo sistem fjalëkalimesh
- Konsideroni përdorimin e një programi menaxher fjalëkalimesh për të ruajtur fjalëkalimet tuaja

Shembull:
Fjalëkalimi: C@tL0v3r#2024
Mnemonika: "Cat Lover at 2024"

MNEMONIKA

Varg nga poezia e Naim Frashërit: **“Ti Shqipëri më ep nderë, më ep emrin Shqipëtar”**

Fjalëkalimi:
T1Shq1p3riM3epNd3r#2024

Mnemonika: **“Ti Shqipëri më ep nder në vitin 2024”**

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

KUR DUHET TË NDËRROHEN FJALËKALIMET?

1. Janë kompromentuar drejtpërdrejt
2. Dyshohen se janë kompromentuar
3. Shfaqen në bazat e të dhënave të shkeljeve të të dhënave online
4. Zbulohen të ruajtura në mënyrë të qartë në një rrjet
5. Zbulohen të transferuara në mënyrë të qartë përmes një rrjeti
6. Ndryshon anëtarsia e një llogarie të përbashkët
7. Nuk janë ndryshuar në 12 muajt e fundit
8. Ka një ndryshim në politikën e sigurisë së organizatës që kërkon përditësimin e fjalëkalimeve

SI TË MBRONI FJALËKALIMET TUAJA

1. Shmangi shkrimin e fjalëkalimit tuaj
2. Përdorni një menaxher fjalëkalimesh me një fjalëkalim kryesor të fortë
3. Shmangni përdorimin e kompjuterëve publikë dhe Wi-FI publik për të hyrë në llogari të ndjeshme (bankë, email, etj.)
4. Mos e lini në vënde ku të tjerët mund ta gjejnë
5. Mos harroni të dilni/logout nga llogaria kur përdorni një kompjuter publik (bibliotekë, internet kafe, ose kompjuter të përbashkët në zyrë)

KONSIDERONI PËRDORIMIN E NJË MENAXHERI FJALËKALIMESH

Aplikacionet menaxhuese të fjalëkalimeve menaxhojnë llogari dhe fjalëkalime të ndryshme duke ofruar edhe përfitime shtesë, përfshirë identifikimin e fjalëkalimeve të dobëta ose të përsërituara.

PËRDORNI PYETJET E SIGURISË SIÇ DUHET

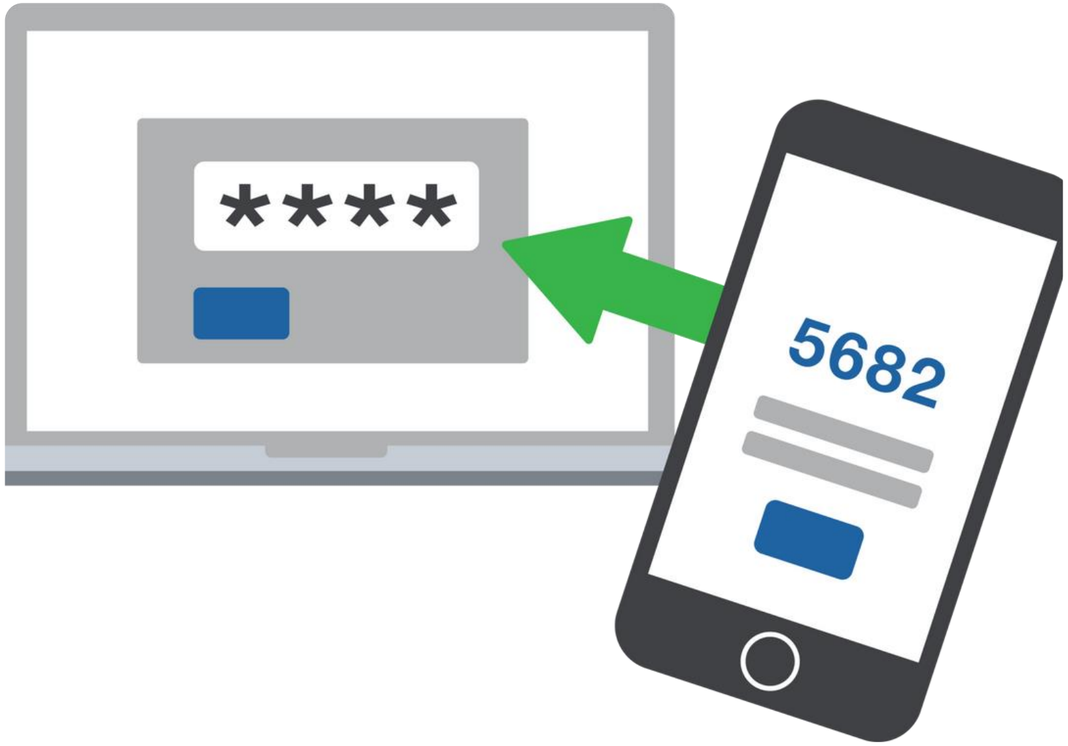
Për llogaritë që ju kërkojnë të vendosni një ose më shumë pyetje për rivendosjen e fjalëkalimit, përdorni informacion privat për veten tuaj që vetëm ju do ta dini.

Përgjigjet mund të gjenden në rrjetet tuaja sociale ose faktet që të gjithë i dinë për ju mund ta bëjnë më të lehtë për dikë që të marrë me mend fjalëkalimin tuaj.

PËRDORNI AUTENTIFIKIMIN ME SHUMË FAKTORË (MFA)

Autentifikimi është një proçes i përdorur për të verifikuar identitetin e një përdoruesi. Sulmuesit shpesh shfrytëzojnë proceset e dobëta të autentifikimit.

MFA përdor të paktën dy komponentë identiteti për të verifikuar identitetin e një përdoruesi, duke minimizuar rrezikun që një sulmues kibernetik të fitojë akses në një llogari nëse din emrin e përdoruesit dhe fjalëkalimin.



INSTALONI NJË FIREWALL

Firewall-et mund të parandalojë disa lloje vektorësh sulmi duke bllokuar trafikun e dëmshëm përpara se të hyjë në një sistem kompjuterik dhe duke kufizuar komunikimet e paneveojshme dalëse.

Disa sisteme operative të pajisjeve përfshijnë një firewall. Aktivizoni dhe konfiguroni si duhet firewall-in sipas udhëzimeve të manualit të pajisjes ose sistemit.

JINI TË DYSHIMTË NDAJ EMAIL-EVE TË PAPRITURA

Email-et phishing janë aktualisht një nga rreziqet më të përhapura për përdoruesit mesatarë.

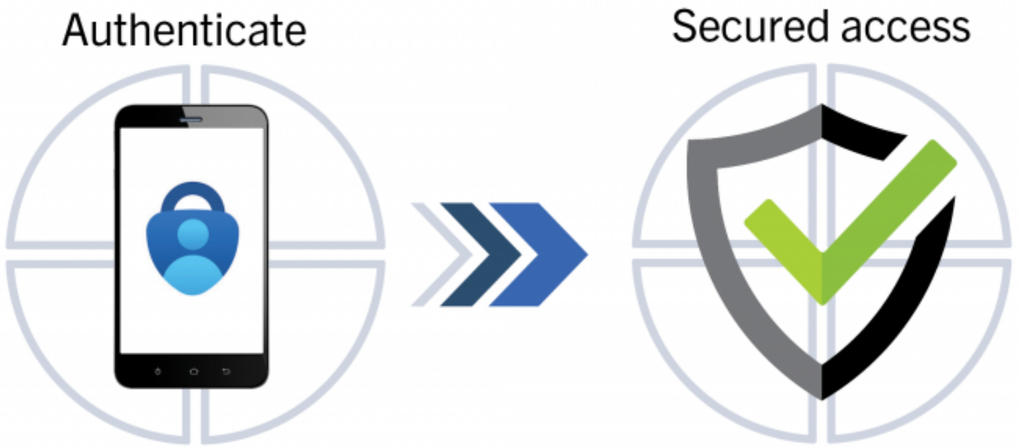
Qëllimi i një email-i phishing është të marrë informacion për ju, të rrëmbejë para nga ju ose të instalojë malware në pajisjen tuaj.

Jini të dyshimtë ndaj të gjitha email-eve të papritura

PSE NUK JANË TË MJAFTUESHME FJALËKALIMET?

Fjalëkalimet janë një shtresë e mirë fillestare e mbrojtjes, por sulmuesit mund t'i marrin me mend ose t'i gjejnë fjalëkalimet. Ne duhet të marrim disa masa shtesë sigurie që mund t'ju mbrojnë edhe nëse një sulmues arrin të ketë fjalekalimin tuaj.

Autentifikimi me shumë faktorë (MFA) është përdorimi i disa pjesëve të informacionit për të verifikuar identitetin tuaj njëkohësisht, dhe po bëhet gjithnjë e më i zakonshëm. (MFA ndonjëherë referohet si 2FA)



KATEGORITË E AUTENTIFIKIMIT

DIÇKA QË DINI

Password*

****

Username
Password
Pyetjet e Sigurisë

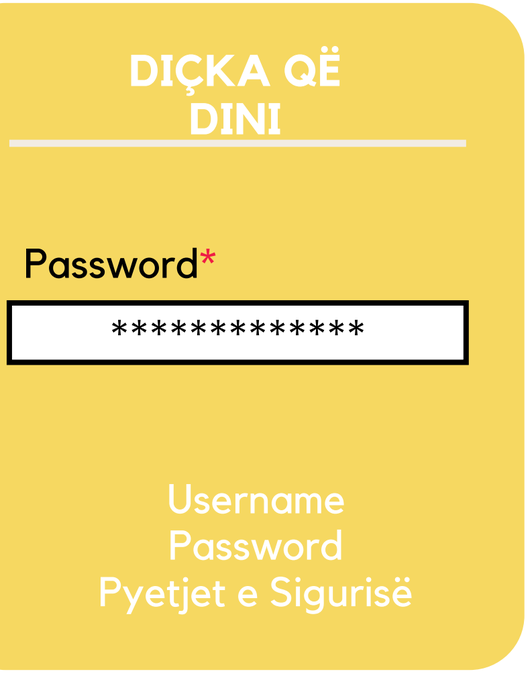
DIÇKA QË KENI

Smartphone
Hardware Key
Smart Card

DIÇKA QË JENI

Fingerprint
Facial Recognition

DIÇKA QË DINI

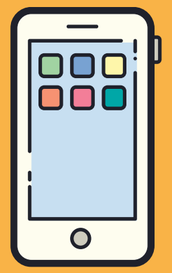


Kjo përfshin fjalëkalimet ose përgjigjet e vendosura paraprakisht për pyetje.

Shmangni zgjedhjen e fjalëkalimeve ose përgjigjeve të lehta, si emri i qenit tuaj, emri i një anatari të familjes, data e lindjes, numrat e telefonit, adresat, etj.

DIÇKA QË KENI

DIÇKA QË KENI



Smartphone
Hardware Key
Smart Card

Kjo mund të jetë një token i vogël fizik si një smart card, një çelës i veçantë, ose një USB. Ju mund të përdorni këtë token në bashkëpunim me një fjalëkalim për të hyrë në një llogari.

Megjithatë, tokenët e bazuar në softuer janë gjithashtu të zakonshëm. Këto tokenë të bazuar në softuer mund të gjenerojnë një numër personal identifikimi (PIN) për përdorim të vetëm për akses. Variacione të tjera përfshijnë mesazhet SMS, telefonatat ose email-et e dërguara përdoruesit me një PIN verifikimi.

DIÇKA QË JENI

DIÇKA QË JENI

Fingerprint
Facial Recognition

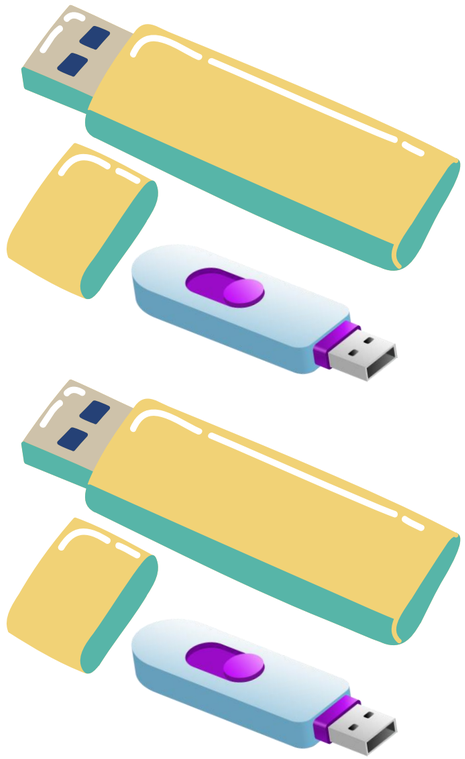
Identifikimi biometrik mund të përfshijë skanimin e syve (retinës ose irisit) ose gjurmëve të gishtave, njohjen e fytyrës, njohjen e zërit ose autentifikimin përmes nënshkrimeve ose lëvizjeve të tastierës.

Një shembull i zakonshëm i identifikimit biometrik është skaneri i gjurmëve të gishtave i përdorur për të identifikuar përdoruesit në shumë smartphone modernë.

CILAT JANË RREZIQET E LIDHURA ME PËRDORIMIN E USB-VE

Disqet USB, ndonjëherë të njohura si thumb drives, janë të vogla, lehtësisht të disponueshme, të lira dhe portative kështu që janë të njohura për ruajtjen dhe transportimin e skedarëve nga një kompjuter në tjetrin. Megjithatë, këto karakteristika të njëjta i bëjnë ato tërheqëse për sulmuesit.

CILAT JANË RREZIQET E LIDHURA ME PËRDORIMIN E USB-VE



- Infektojnë kompjuterët me malware
- Vjedhin informacion direkt në një kompjuter
- Disqet USB mund të humbasin ose të vidhen lehtë
- Çdokush që ka diskun USB mund të ketë askes në të gjitha të dhënat që ka në brendësi

SI MUND TË MBROHENI?

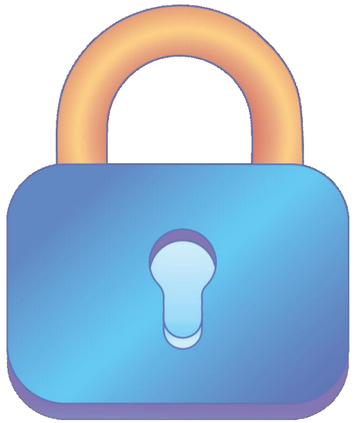
Le të shohim disa hapa që mund të ndërmerrni për të mbrojtur të dhënat në diskun tuaj USB dhe në çdo kompjuter ku mund ta vendosni atë.

MOS VENDOSNI NJË USB TË PANJOHUR NË KOMPJUTERIN TUAJ

Nëse gjeni një disk USB, dorëzojeni tek autoritetet përkatëse (personeli i sigurisë së një vendi, departamenti i teknologjisë së informacionit [IT] të organizatës tuaj, etj.) Mos e vendosni atë në kompjuterin tuaj për të parë përmbajtjen ose për të provuar të identifikoni të zotin e USB.

PËRFITONI NGA MUNDËSITË E SIGURISË

Përdorni fjalëkalime dhe enkriptim në diskun tuaj USB për të mbrojtur të dhënat tuaja dhe sigurohuni që keni bërë kopje rezervë të informacionit në rast se USB-ja juaj humbet.



ÇAKTIVIZONI AUTORUN

Funksioni AutoRun bën që media të lëvizshme, si disqet USB dhe pajisje të tjera të jashtme të hapen automatikisht kur futen në një portë. Duke çaktivizuar AutoRun, mund të parandaloni ekzekutimin automatik të kodit të dëmshëm në një pajisje të infektuar. Kjo ndihmon në mbrojtjen e sistemit tuaj nga kërcenimet e mundshme që mund të futen përmes pajisjeve të lëvizshme të jashtme.

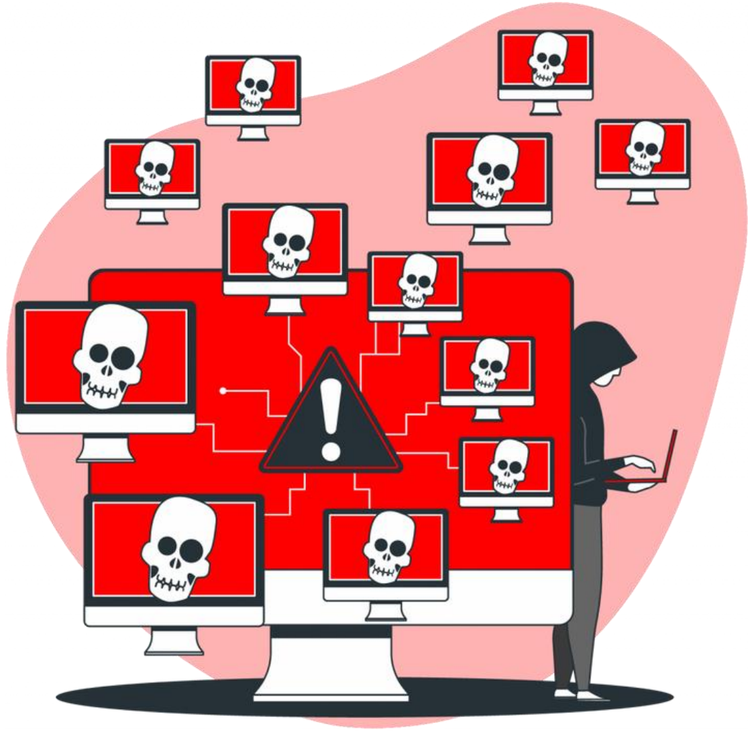
ÇFARË ËSHTË SULMI (DOS)

Një sulm i mohimit të shërbimit (DoS) ndodh kur përdoruesit legjitim nuk janë në gjendje të kenë akses në sistemet e informacionit, pajisjet ose burimet e tjera për shkak të veprimeve të një aktori kërcënues kibernetik të dëmshëm.

Shërbimet e prekura mund të përfshijnë email-e, faqe interneti, llogari online (p.sh. bankare) ose shërbime të tjera që mbështeten në kompjuterin ose rrjetin e prekur. Sulmet DoS mund t'i kushtojnë një organizatë kohë dhe para ndërsa burimet dhe shërbimet e tyre janë të paaksesueshme.

ÇFARË ËSHTË SULMI (DDOS)

Një sulm i mohimit të shërbimit të shpërndarë (DDoS) ndodh kur disa pajisje/kompjutera bashkëveprojnë për të sulmuar një objektiv të vetëm. Sulmuesit DDoS shpesh përdorin një botnet - një grup pajisjesh të lidhura me internetin të kapura për të kryer sulme në shkallë të gjërë. Sulmuesit përfitojnë nga dobësitë e sigurisë ose dobësitë e pajisjeve për të kontrolluar një numër të madh pajisjesh duke përdorur softuer për komandë dhe kontroll (C2)



ÇFARË DUHET TË BËNI NËSE MENDONI SE PO PËRJETONI NJË SULM?

Kontaktoni administratorin e rrjetit tuaj për të konfirmuar nëse ndërprerja e shërbimit është për shkak të mirëmbajtjes ose një çështje të brendshme të rrjetit. Administratorët e rrjetit gjithashtu mund të monitorojnë trafikun e rrjetit për të konfirmuar praninë e një sulmi, të identifikojë burimin dhe të zbusin situatën duke aplikuar rregulla të firewall-i dhe ndoshta duke ridrejtuar trafikun përmes një shërbimi mbrojtjeje DoS

Kontaktoni ofertuesin e shërbimit të internetit (ISP) për të pyetur nëse ka ndërprerje nga ana e tyre ose nëse rrjeti i tyre është objektivi i sulmit dhe ju jeni një viktimë indirekte. Ata mund të jenë në gjendje t'ju këshillojnë për hapat e duhur që duhet të ndërmerrni.

ÇFARË ËSHTË RANSOMWARE

Ransomware është një lloj malware që përdoret nga aktorët kërcënues për të infektuar kompjuterët dhe për të enkriptuar skedarët e kompjuterit deri sa të paguhet një shpërblim.

Pas infektimit fillestar, ransomware do të përpiqet të përhapet në sistemet e lidhura, duke përfshirë disqet e përbashkëta të ruajtjes dhe kompjuterët e tjerë të aksesueshëm.

SI FUNKSIONON RANSOMWARE

Ransomware identifikon disqet në një sistem të infektuar dhe fillon të enkriptojë skedarët brenda çdo disku.

Pasi Ransomware ka përfunduar enkriptimin e skedarëve, krijon dhe shfaq një skedar ose skedarë që përmbajnë udhëzime se si viktima mund të paguajë shpërblimin. Nëse viktima paguan shpërblimin, aktori kërcënues mund të sigurojë një çelës kriptografik që viktima mund të përdorë për të zhbllokuar skedarët, duke i bërë ata të aksesueshëm.

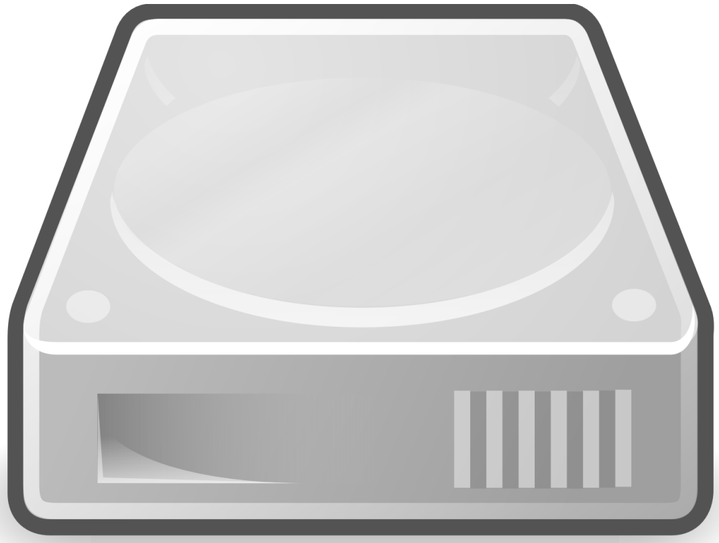
SI INSTALOHET APO INFEKTOHET PAJISJA ME RANSOMWARE?

Ransomware zakonisht dorëzohet përmes email-eve phishing ose përmes “shkarkimeve të rastësishme”. Email-et phishing shpesh duken sikur janë dërguar nga një organizatë legjitime ose dikush i njohur për viktimën dhe nxisin përdoruesin të klikojë në një lidhje të dëmshme ose të hapë një shtojcë të dëmshme.

Një “shkarkim i rastësishëm” është një program që shkarkohet automatikisht nga interneti pa pëlqimin e përdoruesit ose shpesh pa dijeninë e tij. Është e mundur që kodi i dëmshëm të ekzekutohet pas shkarkimit, pa ndërveprimin e përdoruesit.

ÇFARË MUND TË BËNI PËR TË MBROJTUR TË DHËNAT DHE RRJETET TUAJA?

- Krijoni kopje rezervë të kompjuterit tuaj (BACKUP)
- Ruani kopjet rezervë në një vend të sigurt
- Trajnoni stafin e organizatës tuaj



HAPA PËR TË NDIHMUAR NË PARANDALIMIN E INFEKSIONEVE ME RANSOMWARE

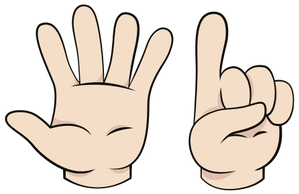
Përditësoni kompjuterin tuaj

Përdorni kujdes me linqet dhe kur vendosni adresa të faqeve të internetit

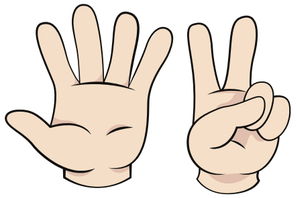
Hapni bashkëngjitjet e email-it me kujdes

Mbani të sigurta informacionet personale

Verifikoni dërguesit e email-it



Informohuni



Përdorni dhe mirëmbani programet parandaluese të softuerit

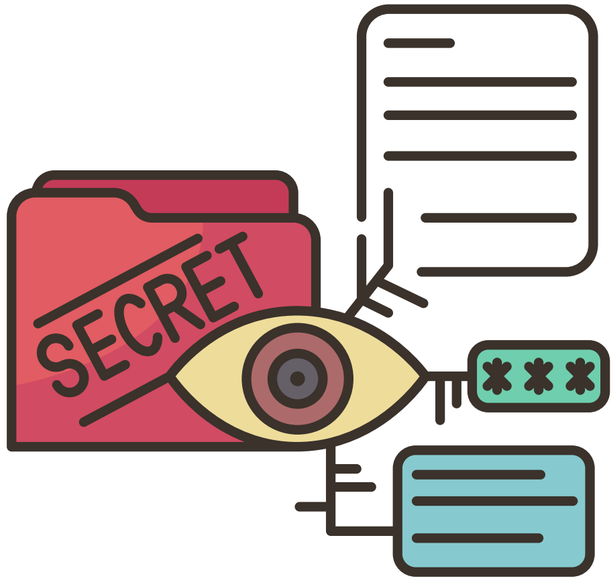
ÇFARË DUHET TË BËNI NËSE KOMPJUTERI JUAJ ËSHTË INFEKTUAR ME RANSOMWARE

1. Ndiqni udhëzimet e AKSK për identifikimin dhe heqjen e ransomware-it. Ekipi jonë ofron burime dhe udhëzime për trajtimin e ransomware-it. Vizition https://aksk.gov.al
2. Këshilltari juaj ligjor mund t'ju ndihmojë të informoni klientët, furnizuesit dhe palët e tjera të prekura për incidentin dhe çdo implikim ligjor.
3. Informoni këdo të prekur nga kompromentimi: Njoftoni stafin, kolegët, familjen dhe miqtë që mund të jenë prekur nga sulmi ransomware.
4. Raportoni incidentin tek AKSK: Ekipi ynë duhet të njoftohet për sulmin Ransomware. Ata mund të ofrojnë ndihmë të mëtejshme dhe të ndjekin kërcënimet kibernetike.
5. Nëse kërkohet nga ligji, raportoni çdo shkelje të të dhënave te Komisionieri për Mbrojtjen e të dhënave Personale.
6. Shmangni përdorimin e Wi-Fi Publik: Për të parandaluar kompromentimie të mëtejshme, mos e lidhni pajisjen e infektuar me rrjetet Wi-Fi publike.
7. Shkëputni pajisjen e infektuar nga rrjeti: Izoloni menjëherë pajisjen nga rrjeti për të parandaluar përhapjen e ransomware-it në pajisje të tjera.
8. Konsultohuni me një profesionist të sigurisë kibernetike: Angazhoni një ekspert të sigurisë kibernetike për të vlerësuar situatën dhe për të ndihmuar në forcimin e masave tuaja të sigurisë për të parandaluar sulmet e ardhshme.

ÇFARË ËSHTË SPYWARE?

Spyware, i njohur gjithashtu si “adware” i referohet një kategorie softueri që, kur instalohet në kompjuterin tuaj, mund të dërgojë reklama pop-up, të ridrejtojë shfletuesin tuaj në faqe të caktuara interneti ose të monitorojë faqet e internetit që vizitoni.

Spyware mund të bëjë që kompjuteri juaj të bëhet i ngadaltë.



A ËSHTË SPYWARE NJË VIRUS?

Spyware dhe viruset kompjuterike janë në të njëjtën familje - të dyja janë lloje të softuerëve të dëmshëm.

Po ka disa ndryshime!

Spyware është një lloj malware që mbledh informacionin tuaj personal dhe grumbullon të dhëna për ju pa pëlqimin tuaj.

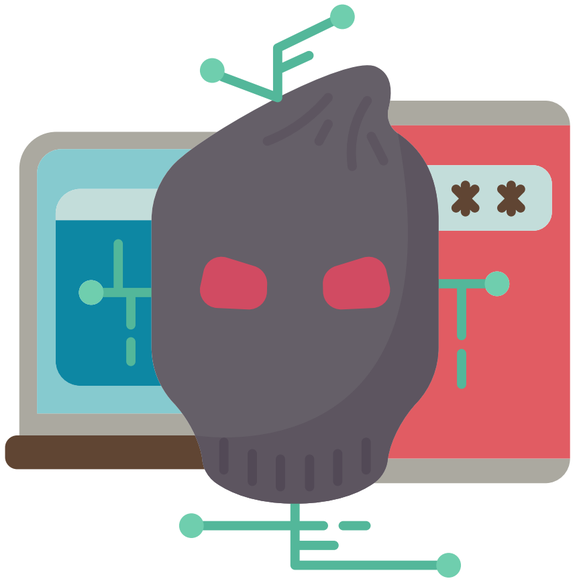
Virusët janë një lloj softueri të dëmshë të krijuar për t'u përhapur nga pajisje të tjera.

IMPLIKIMET E SPYWARE

Për shkak të përpunimit shtesë, spyware mund të bëjë që kompjuteri juaj të bëhet i ngadalësuar ose i paefektshëm,

Ka edhe implikime të privatësisë:

- Çfarë informacioni po mblidhet?
- Kush po e merr atë?
- Si po përdoret ai?



SI E DINI NËSE SPYWARE ËSHTË NË KOMPJUTERIN TUAJ?

1. Ju jeni të ekspozuar ndaj dritareve pop-up të pafundme
2. Ju ridrejtoheni në faqe interneti të tjera përveç asaj që keni shkruar në shfletuesin tuaj
3. Faqja kryesore e shfletuesit tuaj ka ndryshuar papritur
4. Motori i kërkimit që shfletuesi juaj hap kur klikoni “search” është ndryshuar
5. Disa butona nuk funksionojnë në shfletuesin tuaj (p.sh. butoni tab nuk funksionon kur po kaloni në fushën tjetër brenda një forme)
6. Fillojnë të shfaqen mesazhe të rastësishme gabimesh të sistemit operativ
7. Kompjuteri juaj duket papritur shumë i ngadaltë kur hap programe ose kryen detyra si ruajtja e skedarëve, etj.!

SI MUND TA PARANDALONI INSTALIMIN E SPYWARE NË KOMPJUTERIN TUAJ?

- Mos klikoni në linqe brenda dritareve pop-up
- Zgjidhni "jo" kur ju bëhen pyetje të papritura
- Kini kujdes nga softuerët falas të shkarkueshëm
- Mos ndiqni lidhje email-i që pretendojnë të ofrojnë softuer anti-spyware
- Konsideroni të rregulloni preferencat e shfletuesit tuaj për të kufizuar dritaret pop-up dhe cookies

ÇFARË ËSHTË PHISHING?

Phishing është një mënyrë që kriminelët përdorin për të përpjekur të vjedhin informacion të ndjeshëm, si p.sh. detajet e kartës së kreditit, kredencialet e bankës online, frazat e kalimit të biznesit ose fjalëkalimet.

Kjo bëhet duke dërguar mesazhe mashtruese, zakonisht përmes postës elektronike

SI JU MASHTROJNË KRIMINELËT...

Email-et phishing janë dizajnuar që të duken sikur vijnë nga një institucion financiar i vërtetë, një faqe e-commerce, një agjenci qeveritare, ose ndonjë shërbim, biznes, ose individ tjetër.

Email-i mund të kërkojë informacion personal, si numrat e llogarive dhe adresat e email-it.

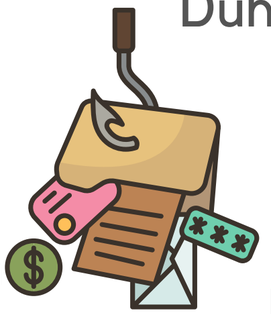
Kur një përdorues përgjigjet në email me informacionin ose klikon në linqe, kriminelët e përdorin këtë për të fituar akses në llogaritë ose kompjuterin personal të përdoruesit.

SHEMBUJ TË MESAZHEVE PHISHING

"Regjistrimet tona tregojnë se llogaria juaj është bllokuar"

"Dyshojmë për një tranksaksion të paautorizuar në llogarinë tuaj"

Duhet të na telefononi brenda 7 ditëve për ta aktivizuar atë.



Për të siguruar që llogaria juaj të mos kompromentohet, ju lutem klikoni në linkun më poshtë dhe konfirmoni identitetin tuaj.

"Gjatë verifikimit tonë të rregullt të llogarive, nuk mundëm të verifikonim informacionin tuaj"

Ju lutem klikoni këtu për të përditësuar dhe verifikuar informacionin tuaj.

DISA METODA QË SHPESH PËRDOREN NË PËRPJEKJET E PHISHING

1. Policia e Shtetit (mashtrime me gjoba të rreme)
2. Shërbime të ndryshme si energjia dhe gazi (fatura të rreme dhe gjoba të vonuara)
3. Shërbimet postale (mashtrime me marrjen e pakove)
4. Bankat (kërkesa të rreme për përditësimin e informacionit tuaj)
5. Shërbimet telekomunikative (fatura të rreme, gjoba ose kërkesa për të konfirmuar të dhënat tuaja)
6. Departamentet qeveritare dhe ofruesit e shërbimeve si Drejtoria e Tatimeve, ISSH dhe e-Albania
7. Institucione arsimore (email-e të rreme për regjitstrim ose pagesa)
8. Shërbimet shëndetësore (kërkesa të rreme për informacion mjekësor ose fatura të rreme)

OPEN SOURCE INTELLIGENCE (OSINT)

Open-source intelligence (OSINT) apo Inteligjenca nga Burimet e Hapura është mbledhja e të dhënave të mbledhura nga burimet të disponueshme publikisht për të prodhuar inteligjencë të përdorshme.

OSINT përdoret kryesisht në:

- Funksionet e Sigurisë Kombëtare
- Funksionet e Zbatimit të Ligjit
- Funksionet e Inteligjencës së Biznesit
- Funksionet e Sigurisë së Informacionit

Është vetëm një tjetër mjet brenda procesit të analistit hetues me teknika të tilla si:

- Intervitsimi
- Mbikëqyrja
- Marrja e gjurmëve të gishtave
- Dhe çdo informacion tjetër publik që është me interes për hetuesin apo analistin i cili mbledh të dhëna

ÇFARË ËSHTË INTELIGJENCA NGA BURIMET E HAPURA - OSINT

Në komunitetin e Inteligjencës (IC), termi "i Hapur" i referohet burimeve të hapura (overt) dhe të disponueshme publikisht, në kundërshtim me burimet "të fsheta" ose (covert) si (përgjimi).

KATEGORITË E BURIMEVE OSINT

Burimet e OSINT mund të ndahen në gjashtë kategori të ndryshme të rrjedhjes së informacionit:

Media: Gazetat e shtypura, revistat, radiot dhe televizioni.

Internet: Publikimet online, bloget, grupet e diskutimit, mediat e qytetarëve (p.sh. - videot e telefonave celularë dhe përmbajtjet e krujuara nga përdoruesit), YouTube dhe faqet e tjera të mediave sociale (p.sh - Facebook, Twitter, Instagram etj..). Ky burim është më i shpejtë dhe më i lehtë për t'u aksesuar krahasuar me burimet e tjera.

Të dhënat publike qeveritare: Raportet publike qeveritare, buxhetet, dëgjimet, konferencat për shtyp, faqet e Internetit dhe fjalëlimet. Edhe pse këto burime vijnë nga një burim zyrtar, ato janë të aksesueshme publikisht dhe mund të përdoren hapur dhe lirshëm.

Publikime profesionale dhe Akademike: Informacioni i marrë nga revista, konferenca, simpoziume, punime akademike dhe teza.

Të dhënat komerciale: Imazhet komerciale, vlerësimet financiare dhe industriale, dhe bazat e të dhënave.

Literatura Gri: Raportet teknike, patentat, dokumenta pune, dokumenta biznesi, punimet e pabotuara dhe buletinet

KATEGORITË E BURIMEVE OSINT

Siguria Kombëtare:

- Përdor OSINT për të monitoruar kërcënimet ndaj sigurisë kombëtare, duke përfshirë terrorizmin dhe spiunazhin.
- Analizon burimet publike për të gjeneruar inteligjencë mbi aktorët shtetërorë dhe jo-shtetërorë që mund të paraqesin kërcënime.
- Përdor informacionet publike për të mbështetur politikën dhe strategjitë e sigurisë kombëtare.

Inteligjenca Ushtarake:

- Përdor OSINT për të mbledhur informacion mbi forcat e armikut, terrenin, dhe operacionet ushtarake.
- Analizon burimet publike për të monitoruar aktivitetet dhe lëvizjet e trupave armike.
- Gjeneron inteligjencë për të mbështetur planifikimin strategjik dhe operacionet taktike.

KATEGORITË E BURIMEVE OSINT

Zbatimi i ligjit:

- Përdor OSINT për të mbledhur prova dhe informacione në hetimet kriminale.
- Ndihmon në identifikimin dhe gjurmimin e aktiviteteve të dyshimta dhe të personave të kërkuar.
- Analizon mediat sociale dhe burime të tjera publike për të mbledhur inteligjencën mbi kriminelët dhe rrjetet kriminale.

Zbulimi Financiar:

- Përdor OSINT për të identifikuar aktivitetet e paligjshme financiare, si pastrimi i parave dhe financimi i terrorizmit.
- Monitoron transaksionet financiare dhe tregjet për të zbuluar anomalitë dhe rreziqet.
- Analizon informacionet publike për të vlerësuar stabilitetin dhe reputacionin e subjekteve financiare.

KATEGORITË E BURIMEVE OSINT

Departamentet e Burimeve Njerëzore:

- Përdor OSINT për të verifikuar informacionit e kandidatëve gjatë proçesit të rekrutimit.
- Monitoron aktivitetet e punonjësve për të siguruar përputhshmërinë me politikat e kompanisë.
- Analizon reputacionin dhe prezencën online të kandidatëve për të marrë vendime më të informuara për punësim.

Siguria e Korporatave:

- Përdor OSINT për të mbrojtur asetet dhe informacionet e kompanisë.
- Monitoron kërcënimet potenciale ndaj sigurisë fizike dhe kibernetike.
- Vlerëson reputacionin dhe rreziqet e lidhura me partnerët dhe konkurrentët.

KATEGORITË E BURIMEVE OSINT

Biznesi i Sigurimeve:

- Përdor OSINT për të zbuluar mashtrimet në sigurime duke hetuar pretendimet e dyshimta.
- Analizon informacionin publik për të vlerësuar rreziqet dhe për të marrë vendime më të informuara për sigurimin.
- Gjeneron profile rreziku për klientët dhe polica të sigurimit.

Akademia dhe Kërkimi Shkencor:

- Përdor OSINT për të mbledhur dhe analizuar të dhëna nga burime të hapura për studime të ndryshme shkencore dhe akademike.
- Analizon burimet publike për të gjeneruar njohuri të reja dhe për të mbështetur hipotezat kërkimore.
- Monitoron trendet dhe zhvillimet në fusha të ndryshme studimore për të qëndruar në përputhje me zbulimet e fundit dhe për të kontribuar në avancimin e njohurive.

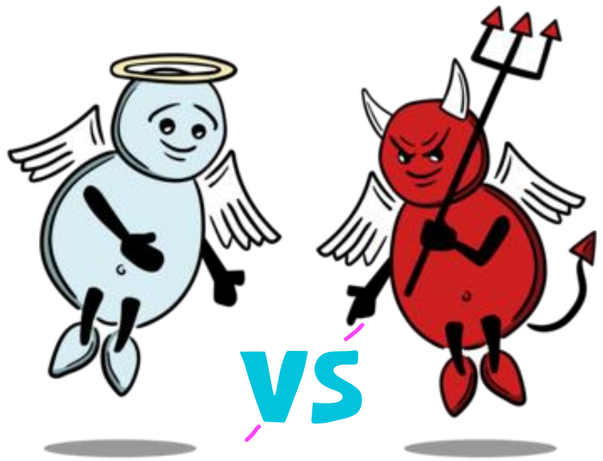
ÇFARË JANË GJURMËT DIGJITALE?

Çfarëdo që lini pas gjatë përdorimit të internetit, çdo gjë që postoni quhet (metadata).

Historia online mund të shihet potencialisht nga njerëz të tjerë ose të gjurmohet në një bazë të dhënash:

- Faqet e internetit dhe blerjet online
- Rrjetet Sociale
- Telefonat mobile
- Tabletat/iPad-ët
- Laptopët/Kompjuterët

LLOJET E PUNËVE PËR OSINT



Për të mirën

- Ndihmon profesionisët e sigurisë të përqëndrohen në zona specifike të interesit.
- Ndihmon njerëzit e kujdesshëm për privatësinë të mësojnë se sa të ekspozuar janë.
- Përdoret për hakerim etik dhe testim penetrimi.
- Ndihmon në identifikimin e kërcënimeve të jashtme.
- Ofron anonimitet gjatë kryerjes së zbulimit pasiv.
- Gjen dhe korrigjon dobësitë në rrjetin e organizatës

Për anën e errët/të keqen

- Aktorët e kërcënimeve kanë akses në të njëjtat mjete dhe teknika si profesionistët e sigurisë.
- Identifikojnë objektiva potencialë dhe shfrytëzojnë dobësitë.
- Ndihmon në sulmet kriminale të phishing dhe fushatat e inxhinierisë sociale.
- Përdoret gjerësisht nga agjencitë e inteligjencës qeveritare.
- Shfrytëzon informacionin e ndjeshëm

OSINT DHE SOCK PUPPETS

Një Sock Puppet është një llogari e rreme ose një identitet i rremë që krijohet nga një individ ose grup për të mashtruar të tjerët.

Këto llogari përdoren shpesh në kontekste të ndryshme, përfshirë OSINT, për të mbledhur informacion pa zbuluar identitetin e vërtetë të përdoruesit.

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.

KEVIN MITNICK: KUMBARI I INXHINIERISË SOCIALE

- (2002) The Art of Deception
- (2005) The Art of Intrusion
- (2011) Ghost in the Wires
- (2017) The Art of Invisibility

Mitnick konsiderohet si një pionier në botën e inxhinierisë sociale, duke e përdorur atë për të fituar akses të paautorizuar në sistemet kompjuterike në vitet 1980 dhe 1990.

Ai nuk ishte një haker tipik që mbështetej në kode komplekse. Pika e Fortë e Mitnick ishte manipulimi njerëzor.

INXHINIERIA SOCIALE ËSHTË ARTI I TRE GJËRAVE

- Manipulimit
- Ndikimit
- Mashtrimit

Inxhinieria sociale është një term që tregon një spektër të gjerë veprimesh keqdashëse të kryera përmes ndërveprimit njerëzor. Inxhinieria Sociale përdor manipulime psikologjike për t'i bërë përdoruesit të zbulojnë informacione konfidenciale ose të bëhen shkak i shkeljeve të sigurisë. Ajo që e bën inxhinierinë sociale veçanërisht të rrezikshme është mbështetja e saj në gabimet njerëzore dhe jo në dobësitë në softuer dhe sistemet operative.

Taktikat e inxhinierisë sociale arrijnë një shkallë suksesi dhjetëfish më të lartë se metodat alternative të sulmit, duke e bërë atë një zgjedhje tërheqëse për hakerat që kërkojnë mjete efikase dhe të besueshme për të shkelur sistemet ose për të marrë informacion të ndjeshëm.

SHUMICA E KOMPANIVE NUK DO TË TELEFONOJNË, DËRGOJNË EMAIL OSE MESAZH DUKE KËRKUAR:

1. Emrin tuaj të përdoruesit, PIN-in, fjalëkalimin ose pytetjet dhe përgjigjet sekrete

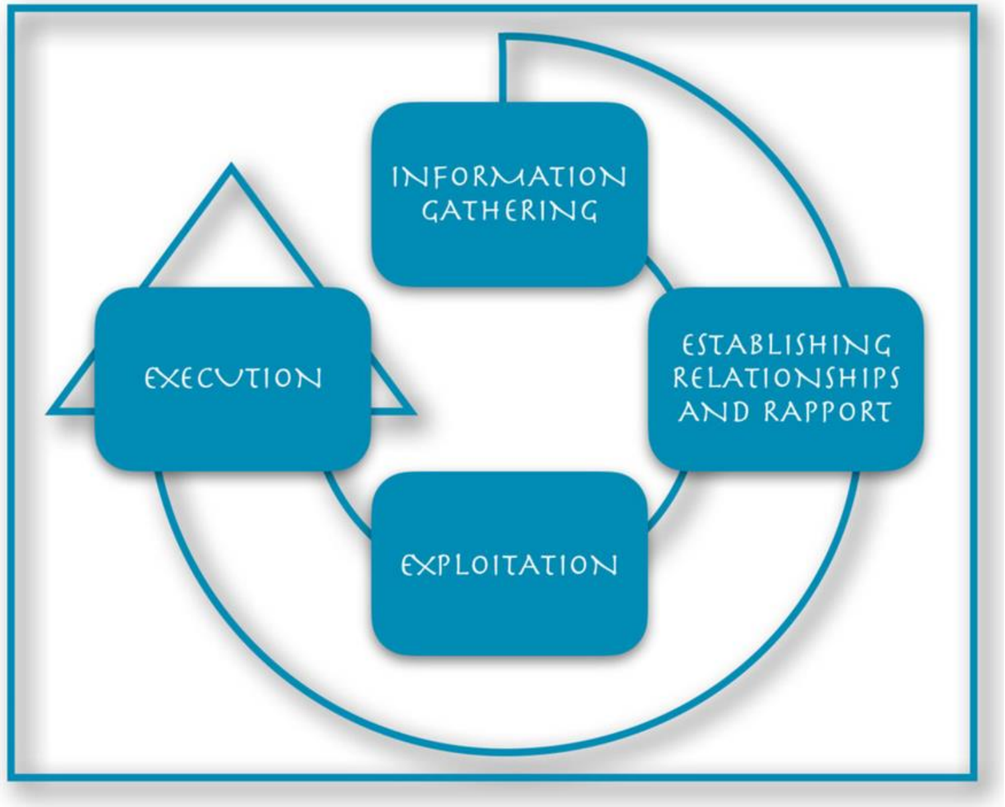
2. Konfirmimin e informacionit personal si detajet e kartës së kreditit ose informacionin e llogarisë

3. Që të vendosni informacion në një faqe web-i që nuk është pjesë e faqes kryesore publike të tyre

4. Kërkimin e pagesës menjëherë (p.sh. për një artikull që nuk është dorëzuar ose një tarifë të vonuar)

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.

Duke luajtur me emocione si:

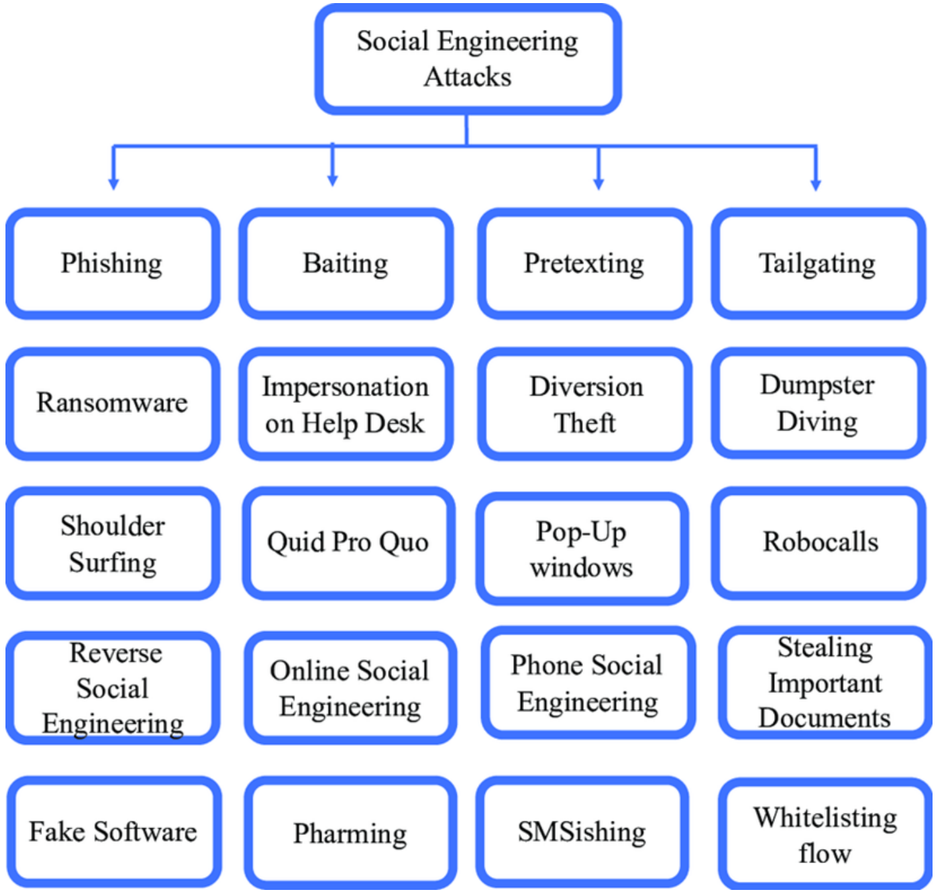
- frikë
- ankth
- zemërim
- trishtim
- euforia
- faji

Besueshmëria:
Kriminelët përgatiten plotësisht për sulmet dhe në mënyrë të besueshme krijojnë mashtrime.

Disa karakteristika kryesore të një Inxhinieri social:

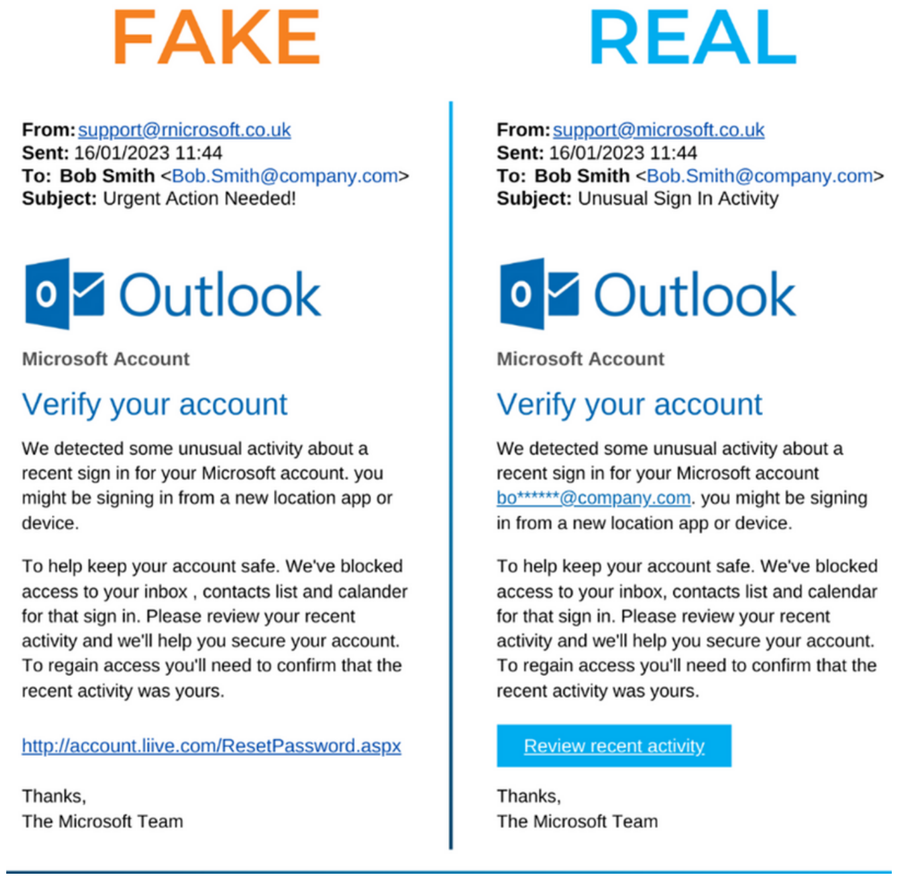
Urgjenca:
Çdo kërkesë që mbështetet nën presionin e kohës. Pavarësisht nëse është një çmim që duhet të kërkohet ose një problem urgjent që kërkon vëmendje të menjëhershme, urgjenca është një shenjë dalluese e inxhinierisë sociale

METODAT E INXHINIERISË SOCIALE



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

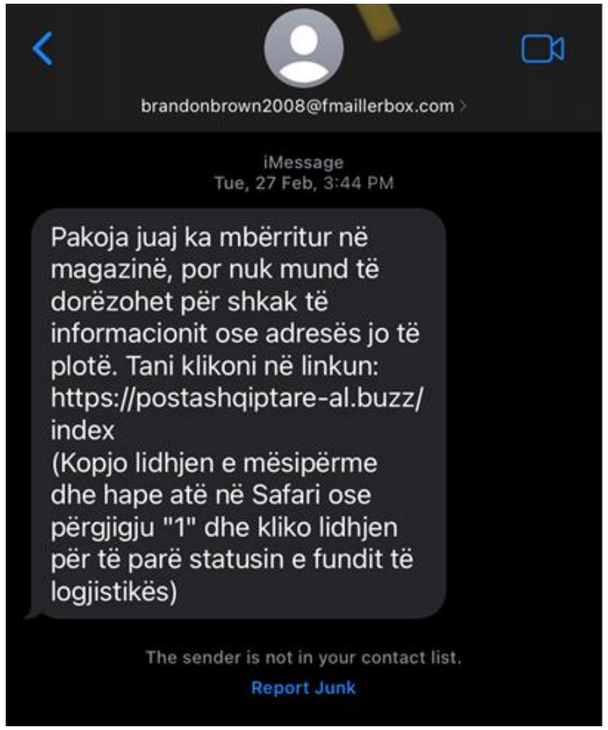
Spear phishing është një mashtrim me email ose komunikime elektronike që targeton/synon një individ, organizatë ose biznes të caktuar.

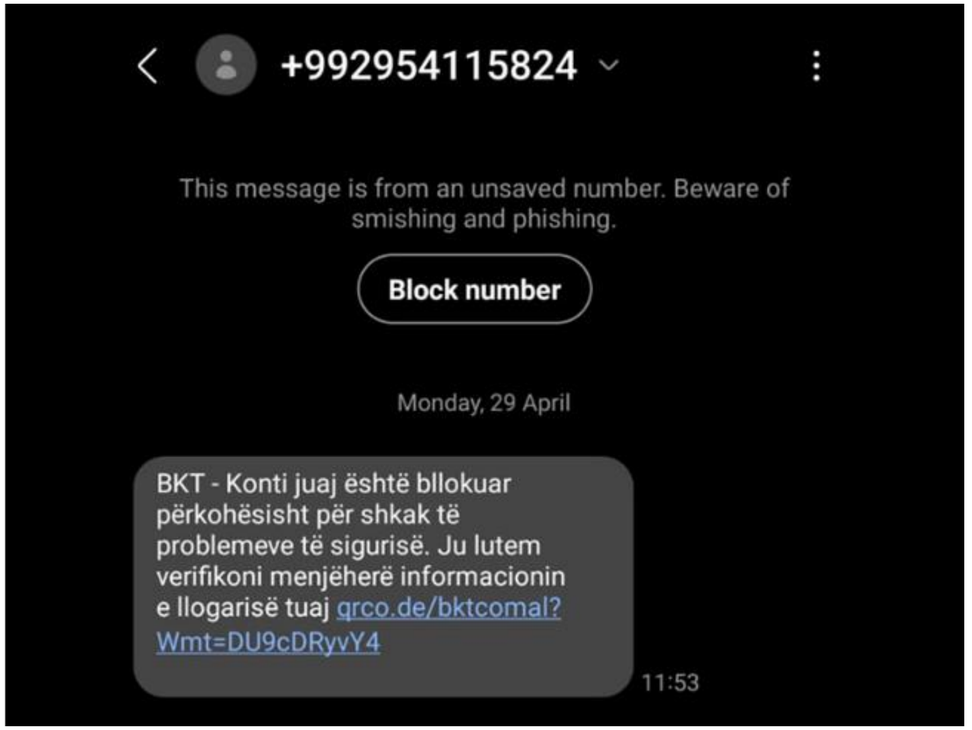
Për shkak të suksesit të sulmeve të phishing, kriminelët kibernetikë kanë zhvilluar një teknikë të rafinuar të njohur si spear phishing. Një email spear phishing është më i synuar se një email i përgjithshëm phishing. Në vend të dërgimit të mijëra email-eve me shpresën për të kapur disa viktima të rastësishme, spear phishing synon njerëz specifikë të profilit më të lartë që kanë akses në diçka që sulmuesi dëshiron.

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



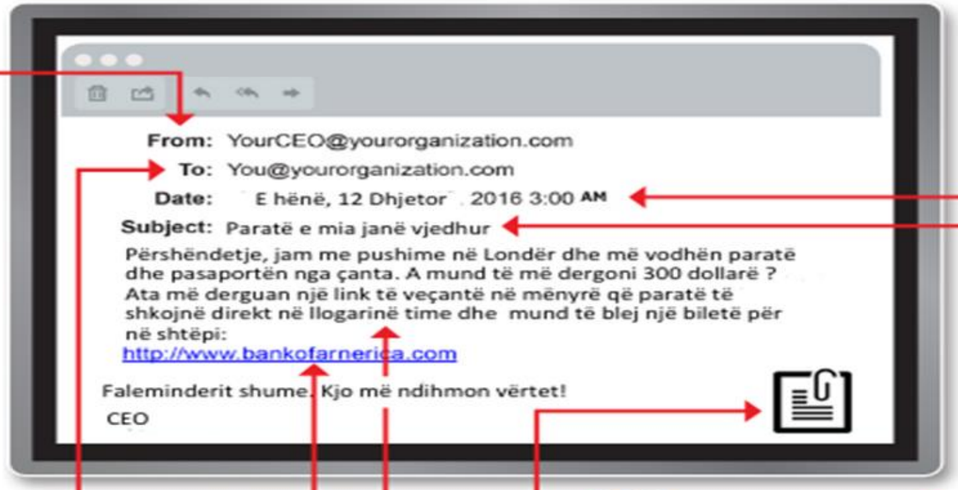


Smishing është një lloj sulmi phishing që përdor inxhinierinë sociale për të marrë informacione personale për dikë nëpërmjet mesazheve me tekst.

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)

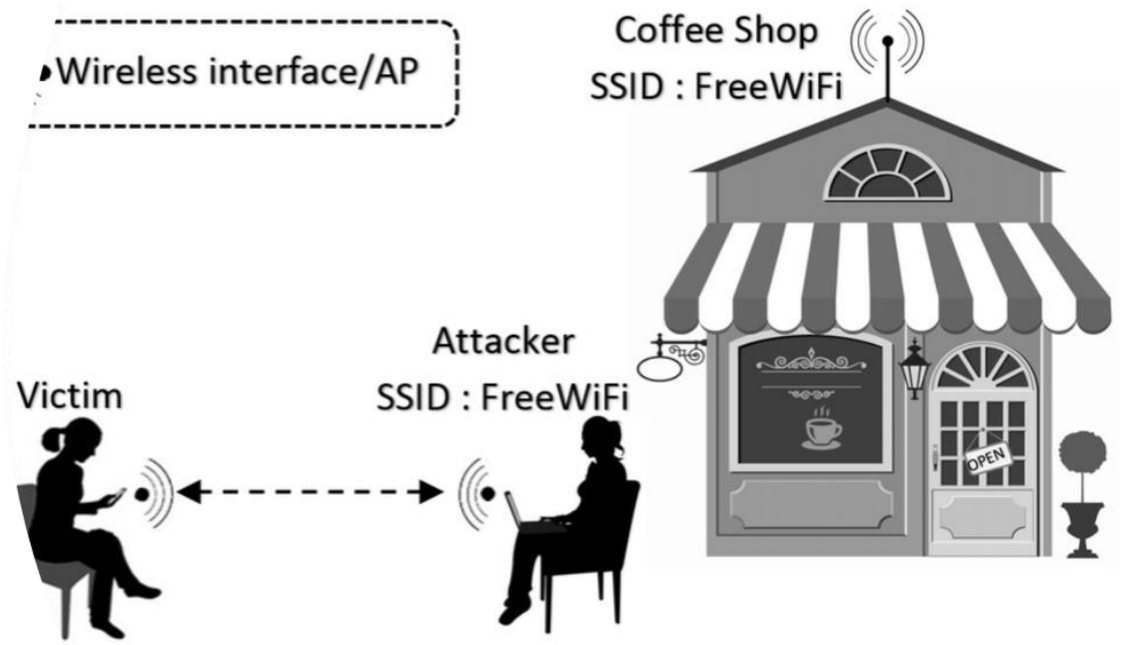
Preteksti: Arti i Tregimit të rremë
Baiting/Karremi: Ofrimi i marrëveshjeve ose promovimeve në dukje tërheqëse

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.

QUID PRO QUO - DIÇKA PËR DIÇKA

Oferta e Sulmuesit: Sulmuesi krijon një pikë të rreme Wi-Fi me një emër që duket legjitim (p.sh., "Wi-Fi falas në aeroport").

Nevoja e Viktimës: Viktima, që ka nevojë për një lidhje interneti, lidhet me hotspot-in e rremë.



Quid Pro Quo: Për të fituar akses në internet, sulmuesi mund t'i kërkojë viktimës të "login" përmes një faqeje të rreme hyrjeje. Kjo faqe e rreme mund të vjedhë kredencialet e identifikimit të viktimës për një rrjet tjetër (p.sh. fjalëkalimin e shtëpisë së tyre Wi-Fi).

KUIZET NË FACEBOOK & Dhurata të kriptomonedhave

Kuizet në Facebook:

Pretekst: Këto kuize shpesh përdorin tituj tërheqës ose pyetje që shkaktojnë kuriozitet ose nostalgji (p.sh., "Cili personazh vizatimor ju pëlqen më shumë?" ose "Testoni njohuritë tuaja për vitet '90!"). Ata e pozicionojnë veten si një mënyrë argëtuese dhe e padëmshme për të kaluar kohën.

Karremi: Pasi të filloni kuizin, mund t'ju bëhen pyetje në dukje të padëmshme për veten tuaj, preferencat tuaja apo edhe ditëlindjen tuaj.

Mbledhja e të dhënave: Këto pyetje në dukje të pafajshme janë në fakt një mënyrë për krijuesit e kuizit për të mbledhur informacione personale për ju. Këto të dhëna më pas mund të përdoren për reklama të targetuara, t'u shiten palëve të treta ose madje të përdoren për të nisur sulme më të hollësishme të inxhinierisë sociale.

Shqetësimet e privatësisë: Shumë kuize në Facebook kërkojnë që ju t'u jepni atyre akses në informacionin e profilit tuaj ose listën e miqve. Kjo mund t'u japë atyre akses në edhe më shumë të dhëna personale dhe mund t'i ekspozojë miqtë tuaj në të njëjtin kuiz.

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

Të skanosh apo të mos skanosh?

SI TË IDENTIFIKONI NJË INXHINIER SOCIAL?

- Aktivitete të nxituara
- Përdor elementin Frikë
- Vëzhgoni për gabime të vogla drejtshkrimore

- Nuk jep informacion kontakti
- Kërkon gjithmonë informacione të ndaluara

SI TË SHMANGNI QË TË BËHENI VIKTIMË?

1. Jini të dyshimtë ndaj telefonatave të papritura, mesazheve sms apo email nga individë që kërkojnë informacione rreth punonjësve ose informacione të tjera të brendshme

2. Mos jepni informacione personale ose informacione rreth organizatës suaj, përveç kur jeni të sigurtë për autoritetin e personit që kërkon informacionin.

3. Mos zbuloni informacione personale ose financiare në email dhe mos u përgjigjni kërkesave për këtë informacion nëpërmjet emailit. Kjo përfshin ndjekjen e linqeve të dërguara në email

4. Instaloni dhe mirëmbani programe anti-virus, firewall dhe filtra për çdo email.

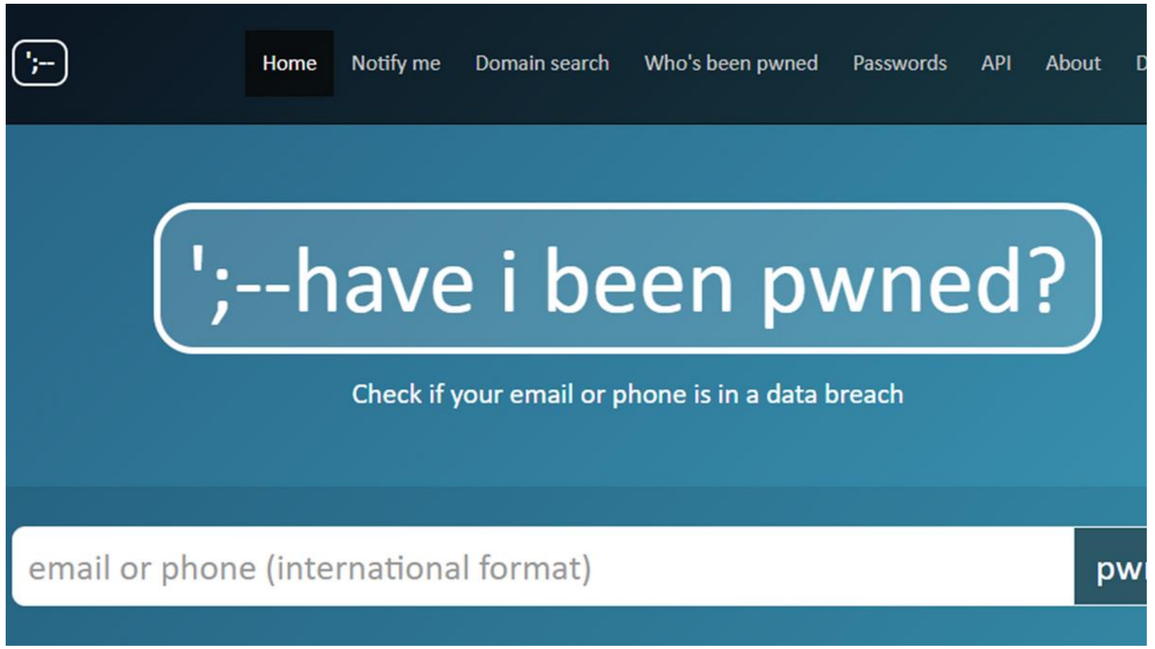
5. Përfitoni nga çdo funksion anti-phishing që ofrohet nga klienti juaj i emailit dhe shfletuesi i internetit.

6. Zbatoni autentifikimit me shumë faktorë (MFA)

7. Mos dërgoni informacione të ndjeshme në internet para se të kontrolloni sigurinë e faqes Web.

8. Verifikoni kërkesën duke kontaktuar drejtëpërdrejt kompanitë duke përdorur detajet e kontaktit nga deklaratat e mëparshme

HAVE I BEEN PWNED?



Have I Been Pwned (HIBP) është një faqe interneti falas që ju lejon të kontrolloni nëse adresa juaj e emailit ose numri i telefonit është përfshirë në një shkelje të të dhënave.

Faqja e internetit gjurmon shkeljet e të dhënave nga një sërë burimesh, duke përfshirë kompanitë, qeveritë dhe studiuesit e sigurisë.

FALEMINDERIT PËR VËMENDJEN!

https://aksk.gov.al