# “Siguria kibernetike sot: Rreziqet reale dhe mbrojtja e përditshme”

# QËLLIMI

## 01 Informim

Siguria kibernetike fillon me informimin

## 02 Ndërgjegjësim

Rritja e ndërgjegjësimit publik


## 03 Mbrojtje

Ofrimi i njohurive praktike për mbrojtjen në hapësirën digjitale

## 04 Rëndësia

Realiteti: teknologjia e pranishme në çdo aspekt të jetës sonë personale/profesionale, njohja e rreziqeve kibernetike dhe zbatimi i masave mbrojtëse janë thelbësore për ruajtjen e sigurisë së të dhënave dhe privatësisë.

# AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE (AKSK)


**Misioni:** **arritja e një niveli të lartë të sigurisë kibernetike**

Përcaktimin e masave të nevojshme të sigurisë, të drejtave dhe detyrimeve të subjekteve
Promovimin e bashkëpunimit të ndërsjellë ndërmjet aktorëve që operojnë në këtë fushë
https://aksk.gov.al

**Ligji:** **nr. 25/2024 "Për Sigurinë Kibernetike"**

https://aksk.gov.al/wp-content/uploads/2024/05/ligj-2024-03-21-25-5-1.pdf

# SECURITY OPERATIONS CENTER (SOC)


## Pjesë e CSIRT kombëtar në AKSK

- Funksion drejtues / koordinues në nivel kombëtar për aktivitetet e reagimit ndaj incidenteve të sigurisë kibernetike.
- Përgjegjës: menaxhimin e incidenteve me ndikim kombëtar, bashkëpunimin ndërkombëtar dhe standardizimin e praktikave të reagimit ndaj incidenteve kibernetike.
- https://aksk.gov.al/wp-content/uploads/2025/07/Rregullore-Funksionimi-Teknik.pdf

## Sektori i Monitorimit dhe Reagimit të Incidenteve Kibernetike

- Vija e parë e mbrojtjes (centralizuar) kibernetike për infrastrukturat Kritike / Rëndësishme
- 24/7: ne kohe reale - monitorim, detektim, analize dhe reagim ndaj incidenteve kibernetike
- Siguri proaktive: skanime passive, identifikim vulnerabilitetesh, threat hunting
- https://aksk.gov.al/wp-content/uploads/2025/06/4.11.24-Procedura-e-Menaxhimit-te-Incid.-te-Sig.-se-Inf-Playbooks-tetor-2024_2.pdf
- https://aksk.gov.al/wp-content/uploads/2024/08/Kategorizimi-i-incidenteve-te-sigurise-kibernetike-21.08.2024.pdf

# TEMAT KRYESORE

01 Siguria kibernetike në jetën e përditshme – koncepti dhe rëndësia

02 Siguria kibernetike në ambientin e punës

03 Siguria kibernetike në jetën personale.

04 Siguria kibernetike në shtëpinë inteligjente (Smart Home)

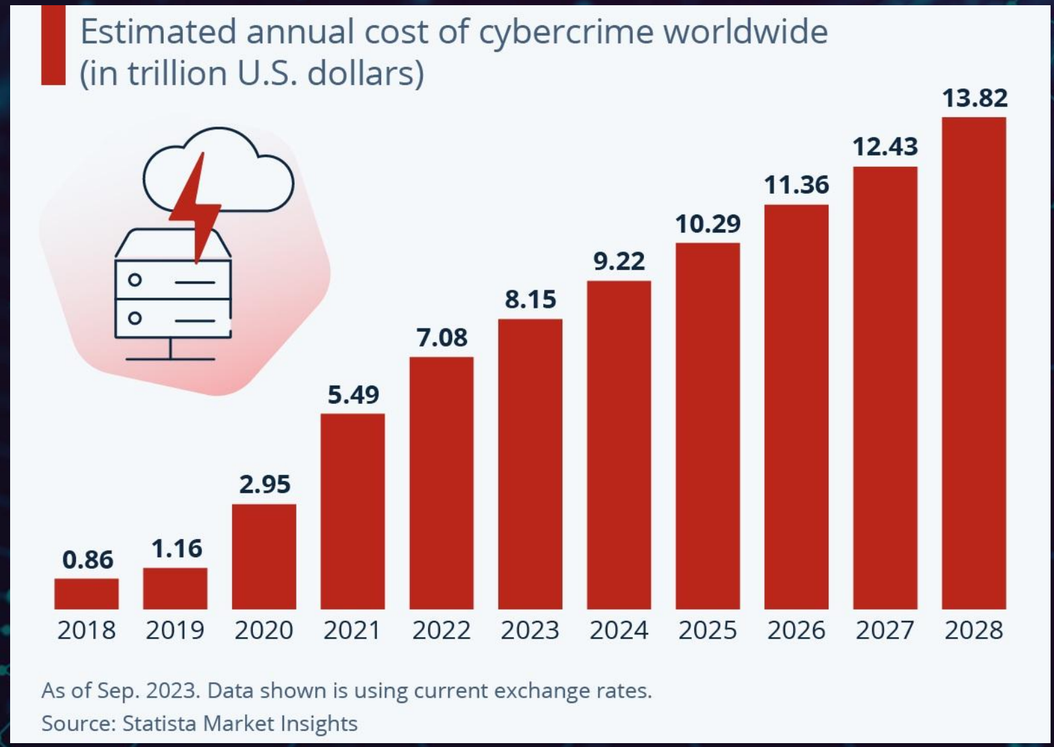
# SIGURIA KIBERNETIKE NË JETËN E PËRDITSHME  KONCEPTI / RËNDËSIA

**Koncepti: mbrojtja e sistemeve kompjuterike, rrjeteve, pajisjeve, aplikacioneve dhe të dhënave nga sulmet digjitale (aksesi i paautorizuar, dëmtimi apo vjedhja e informacionit)**

- Qëllimi kryesor: garantimi i CIA (Konfidencialitet, Integritet, Disponueshmëri)
- Ke prek: të gjithë njerezit (qytetarë/punonjës)
- Kur: sot, në cdo moment dhe cdo ditë të jetës së përditshme
- Si: mënyra të ndryshme, të thjeshta / sofistikuara

## Rëndësia:

- Kostoja globale e krimit kibernetik: pritet të arrijë $13.82 trilion deri në 2028
- Kercenime te reja: 560,000 malware çdo ditë në të gjithë botën
- Perdorimi i AI: 87% bizneseve shqetësohen për AI në sulmet kibernetike
- Jo luks teknologjik: siguri profesionale/personale
- Do na ndodh !? jo pyetje nëse do të na ndodhë ndonjehere sulm, por kur?



# SIGURIA KIBERNETIKE “SOT”

**Vetëm çështje IT !?** çështje jetës së përditshme të çdo punonjësi/qytetari, të gjithë jemi pjesë e ekosistemit digjital

**Fillimi i nje incidenti:** shpesh jo nga teknologjia e avancuar, por një gabim i vogel në përdorimin e përditshëm të pajisjeve, mungesa e praktikave bazë të sigurisë.

**Kufiri jetë profesionale - personale:** është zhdukur, një pajisje mund të përdoret për punë dhe për gjëra personale, kompromet imi personal ->rrezik institucional

**Vetëm kompjuteri i punës !?** çdo pajisje e lidhur në internet përbën një pikë rreziku

# SIGURIA KIBERNETIKE NË AMBIENTIN E PUNËS

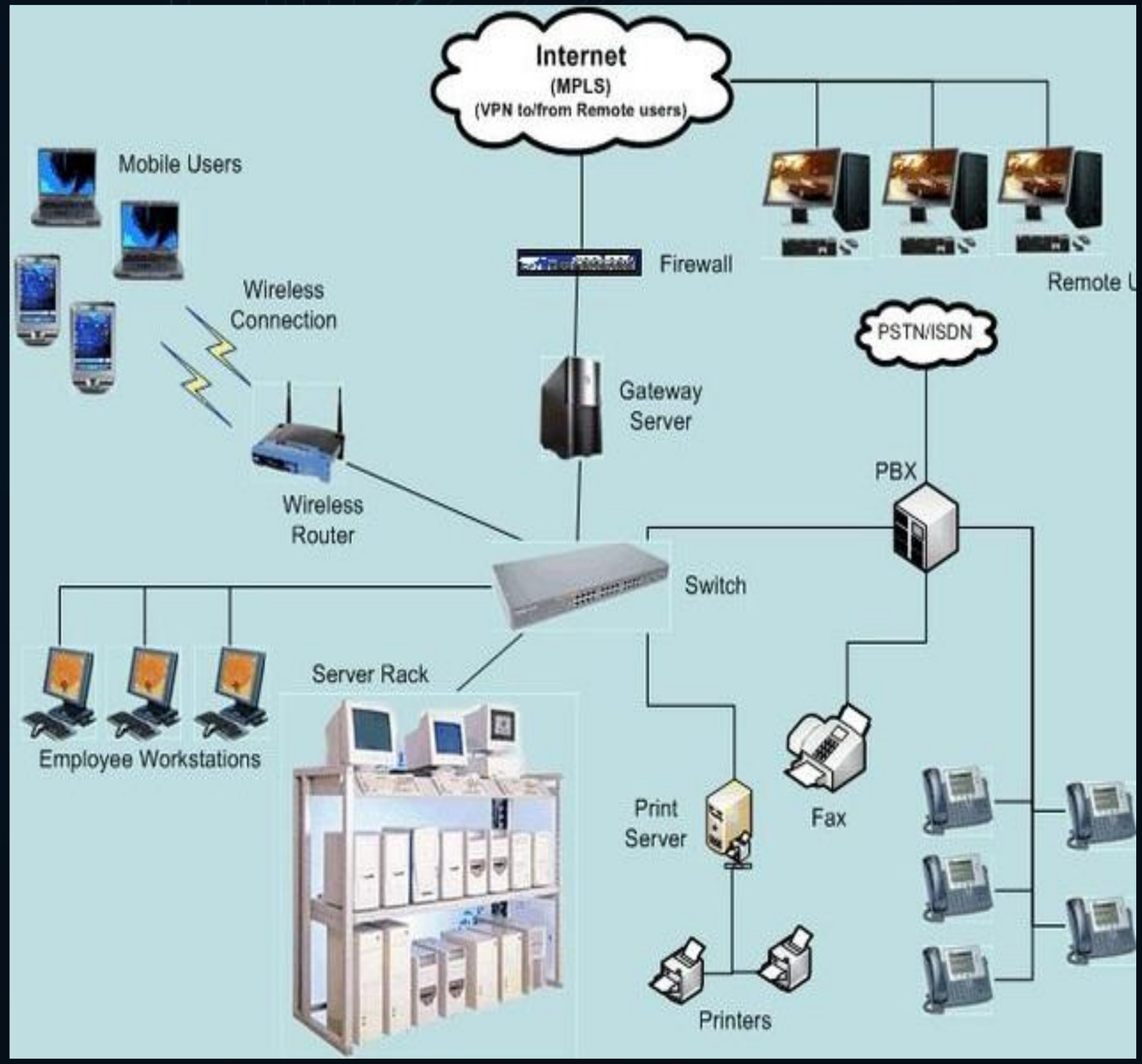
## Institucionet publike objektiv madhor?

**Përpunojnë të dhëna sensitive**

**Ofrojne sherbime publike kritike**
energji
shendetesi
ujesjelles

**PC pune kompremetuar?**
“porte” hyrese
kompromentim gjithe rrjetit

**Pasojat**
humbje te dhenash
nderprerje sherbimesh
demtim reputacioni



# SULME KIBERNETIKE


PHISHING

BRUTE FORCE

MALWARE

RANSOMWARE

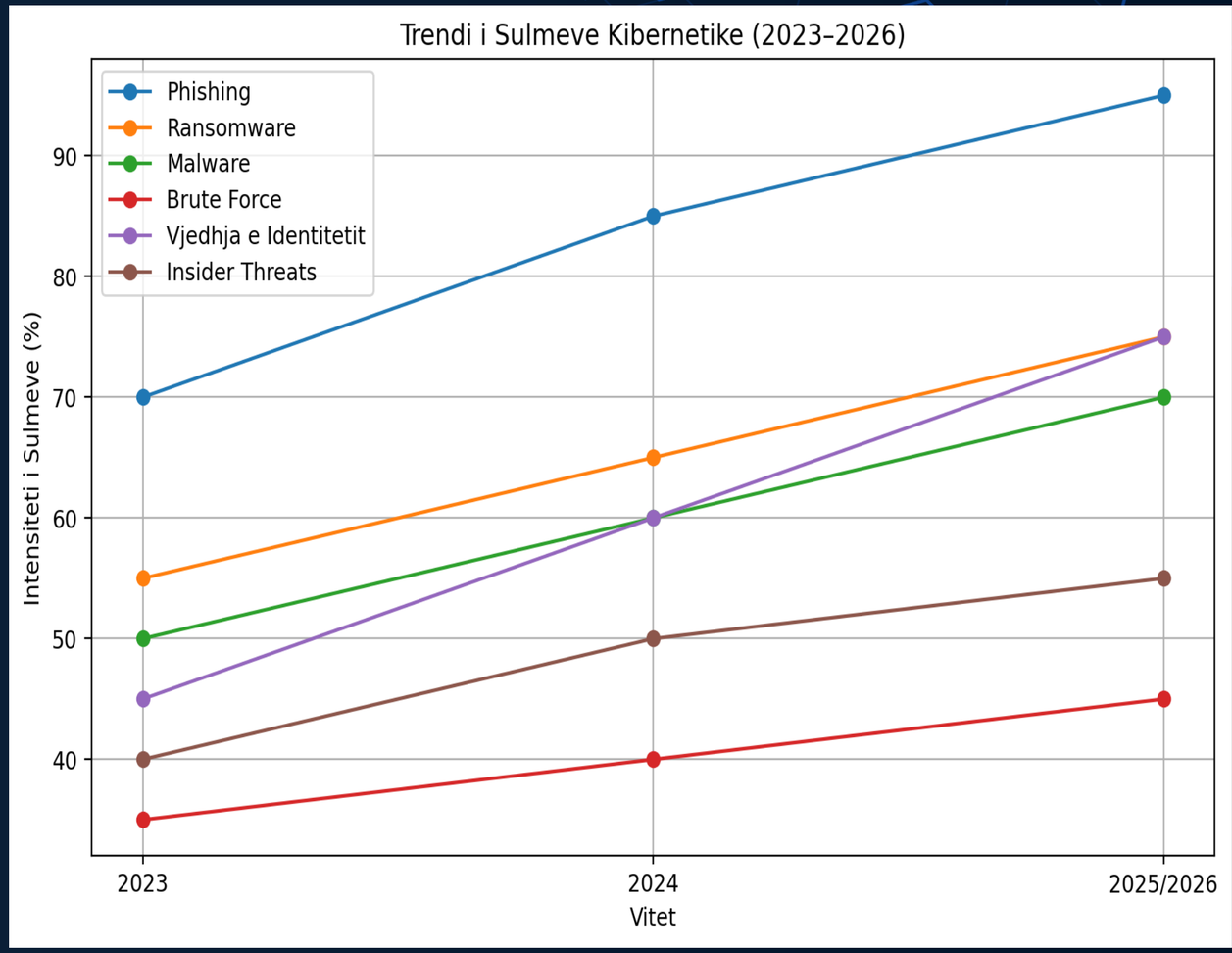
VJEDHJA

IDENTITETIT

DDOS


INSIDER

THREATS



# SULMET KIBERNETIKE

## Phishing


**Qëllimi:**
- vjedhja fjalekalimeve
- hapi pare i një sulmi të madh

**Karakteristika:**
- email i papritur
- link i dyshimtë
- kërkesa për fjalëkalim
- urgjenca artificiale
- gabime drejtshkrimi

**Mbrojtja:**
- mos kliko link të dyshimtë
- mos shkarko attach dyshimtë
- kontrollo dërguesin
- konfirmim / kontakto dërguesin
- raportim IT / AKSK

# SIGURIA KIBERNETIKE NË PUNË – PUNONJËSI

01

## Edukimi dhe vetëdija

Trajnime
Njohja paralajmerimeve

02

## Menaxhimi i fjalëkalimeve

Te forta
Unike
Ndrysho cdo pak muaj
Menaxher fjalëkalimesh te certifikuar
Mos i ndaj me te tjere
Dyshim kompromentimi: ndrysho menjehere

03

## Autentifikimi MFA

Dy ose më shumë forma verifikimi
Hap shtesë mbrojtje
Email, nr. Telefoni
Aplikacion Microsoft/Google Authenticator
Te dhena biometrike
Në cdo llogari (sensitive, bankare)

04

## Mbrojtja të dhënave sensitive

Jo diskutim ne public
Kanale te sigura komunikimi
Kycja/fikja e PC

# SIGURIA KIBERNETIKE NË PUNË – PUNONJËSI



## Karakteristika fjalekalim i forte

- Të paktën 12 karaktere
- Shmangni fjalëkalimet e zakonshme
- Përzierje të karaktereve
- Unike për çdo llogari
- Jo info personal (emer, data lindjes)

# SIGURIA KIBERNETIKE NË PUNË – INSTITUCIONI (PUBLIK/PRIVAT)

01

## Kontrollet e aksesit

Punonjesi sa me pak privilegje/akses

02

## Përditësimet e Sigurisë

Te rregullta
Shfrytezohen dobesite e pajisjeve
Rregullime kritike te sigurise
Automatike
SO, Office, antivirus, ejt

03

## Mbrojtja e rrjetit

Firewall: kontroll trafikun hyrës/dalës
SIEM: monitorim logeve/alerte
Segmentimi rrjeti: izolo sistemet kritike
EDR/XDR
Antivirus
Mbyllje “portave” / sherbimeve akses jo nevojshem ne internet
VPN per akses “remote”

04

## Kopje rezerve / rikuperim

Backup & Recovery
Kopje të rregullta të automatizuara
Testo aftesine e rikuperimit
Mbrojtje ransomware: izolo kopje
Strategjia 3-2-1: 3 kopje-2 media të ndryshme-1 jashtë lokacionit

# SIGURIA KIBERNETIKE NË PUNË – INSTITUCIONI (PUBLIK / PRIVAT)

06

## Plani reagimit ndaj incidenteve

Cikli Menaxhimit të Incidentit Kibernetik (AKSK, NIST)
Rregullore AKSK
Ndihmon në minimizimin e demit

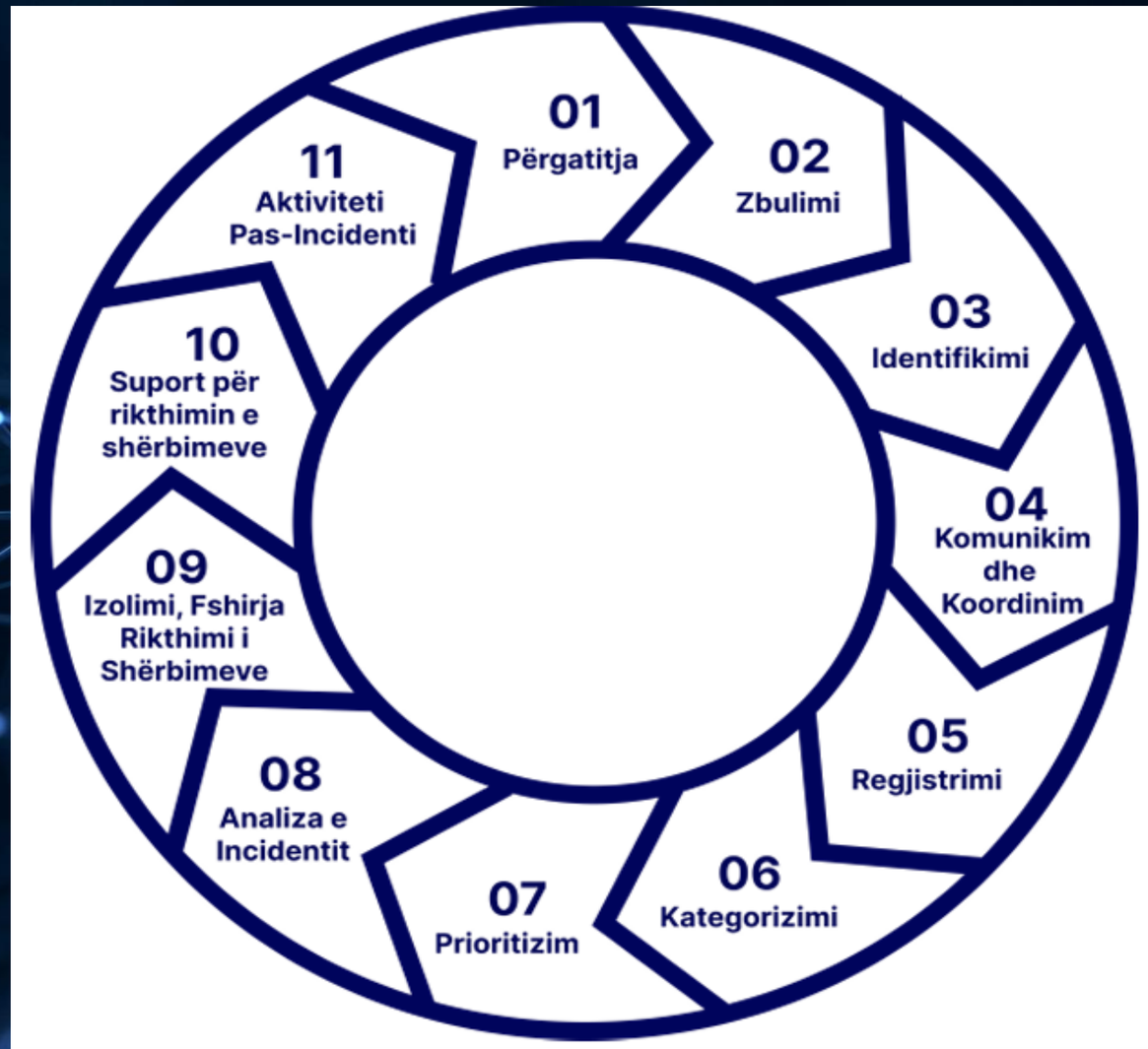
05

## Sigurimi rrjetit Wi-Fi

Ekspozuar ne public
Punonjesit lidhin tel. personal
Rrezik “porte hyrese”
Konfiguro settings (jo default)
Password te forte/unik
Hide SSID
Aktivizo enkriptimin me te fundit
Perditeso rregullisht firmware
Ndaj rrjetin wi-fi nga rrjetet e tjera, virtualisht/fizikisht.

## SOC

Zbulimi i incidentit kibernetik
Identifikimi i incidentit kibernetik
Komunikimit dhe kordinimi me infrastrukturat
Kategorizimi i incidentit
Prioritizimi i incidentit
Analiza e incidentit
Izolimi incidentit, rikthimi i shërbimit



# SIGURIA KIBERNETIKE NË PUNË - INSTITUCIONI (PUBLIK / PRIVAT)

## Komunikim + Bashkëpunim + Raportim

- AKSK / SOC
- 24/7 (në kohë reale)
- Plotësimi pyetësorit paraprak
- Ndihmë: playbook AKSK “Menaxhimin e Incidenteve të Sigurisë Kibernetike”
  https://aksk.gov.al/playbooks

**Pyetësori paraprak i ekspertit të SOC T1 drejt pikës së kontaktit të infrastrukturës:**

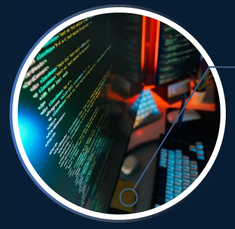
a. Cila është kategoria e incidentit që dyshoni se ka ndodhur?
b. Cili është statusi aktual i incidentit?
    a. Po ndodh
    b. Po ndodh dhe është nën kontroll
    c. Ka ndodhur dhe është nën kontroll
    d. Ka ndodhur
c. Kur është evidentuar incidenti?
d. Si është evidentuar incidenti?
e. A janë prekur sisteme/shërbime nga ky incident?
    a. Nëse po, cilat sisteme/shërbime janë prekur?
        i. A ka shërbime kritike të prekura?
f. Cilat janë masat e marra deri më tani?
g. A dispononi SIEM?
    a. Nëse po, kontrolloni log-et për evente të dyshimta.
h. Kontrolloni Antivirusin.
i. A janë zbuluar indikatorë të incidentit (Indikatorët e Kompromentimit)?
    a. A keni identifikuar skedarë të infektuar/përdorues të rinj të krijuar?
    b. A keni identifikuar trafik të dyshimtë (IP/Domain) ose volum të trafikut të krijuar si pasojë e eksfiltrimit apo DoS/DDoS?
    c. A keni identifikuar email të dyshimtë?
j. A janë prekur institucione/degë të tjera me të cilat ju keni lidhje të drejtpërdrejtë?

# KËRCËNIMET E AVANCUARA KIBERNETIKE


SULMET E FUQIZUARA ME AI

SULMET NË ZINXHIRIN E FURNIZIMIT

KËRCËNIMET E INFORMATIKËS KUANTIKE



DOBËSITË ZERO-DAY

# SIGURIA KIBERNETIKE NË JETËN PERSONALE

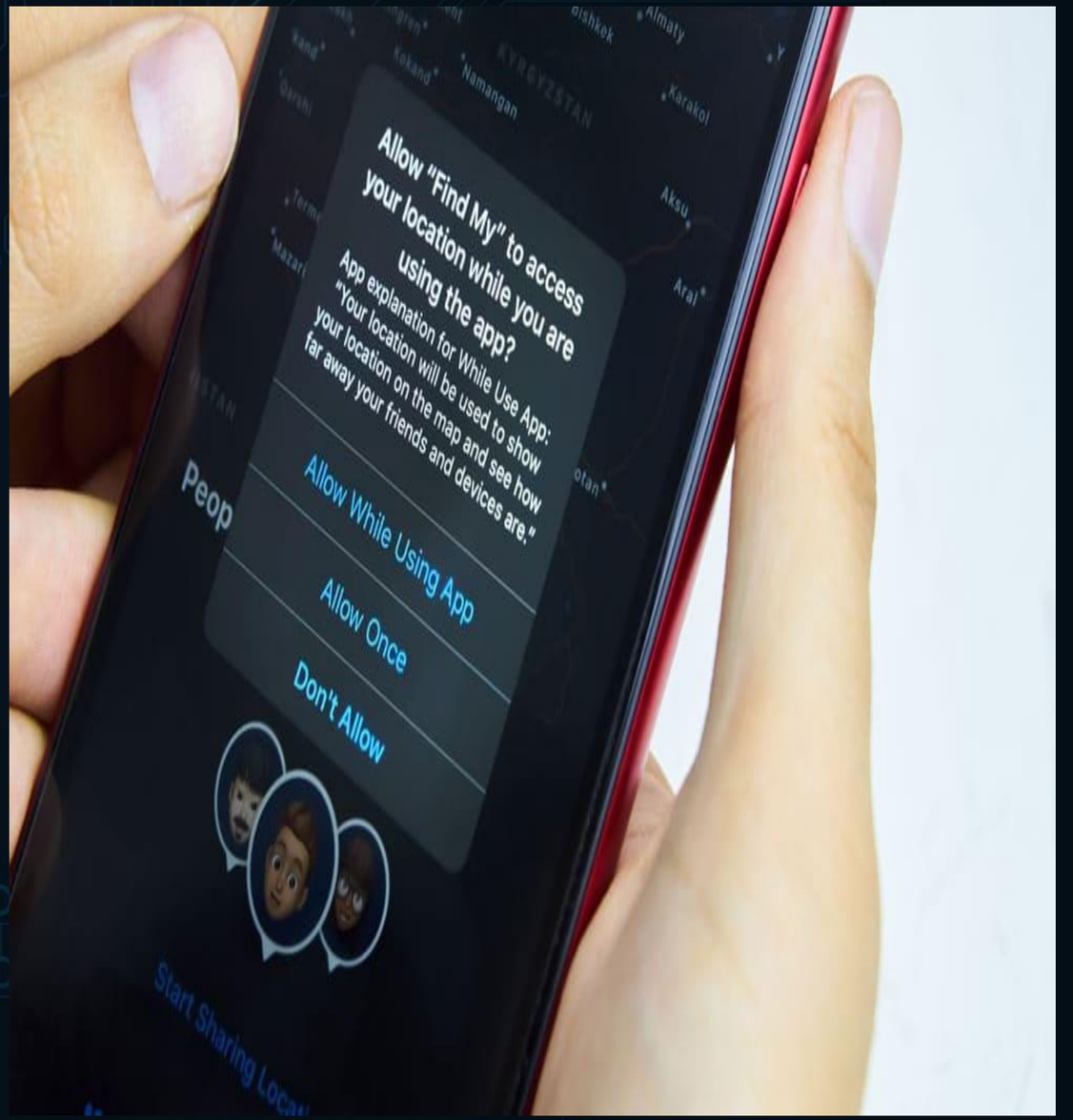
Telefoni inteligjent = kompjuter personal?

(+) Pajisja jonë më inteligjente/perdorur

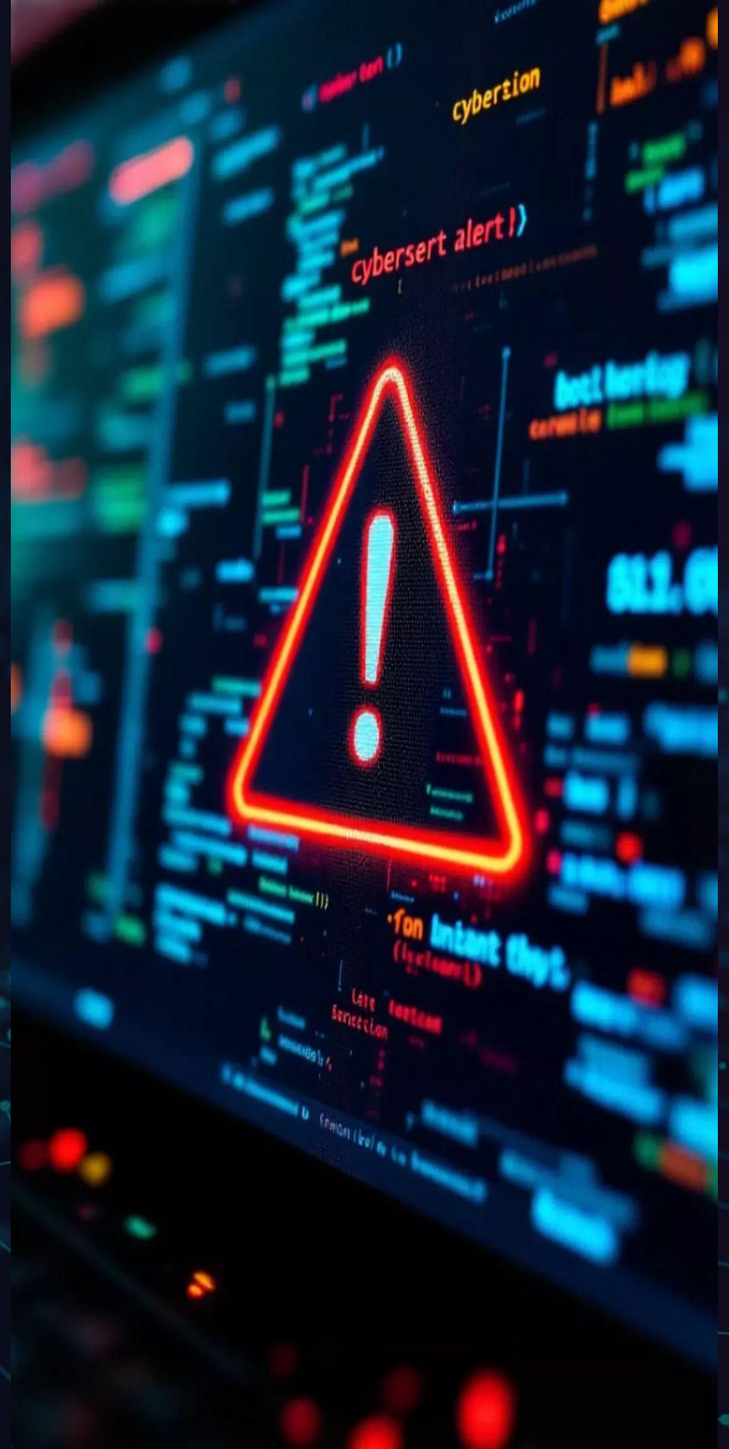
(-) Pajisja më e ekspozuar ndaj rreziqeve kibernetike

Kamera, mikrofon, kontakte, email-e, dokumente, aplikacione pune/private

‘App permissions’?

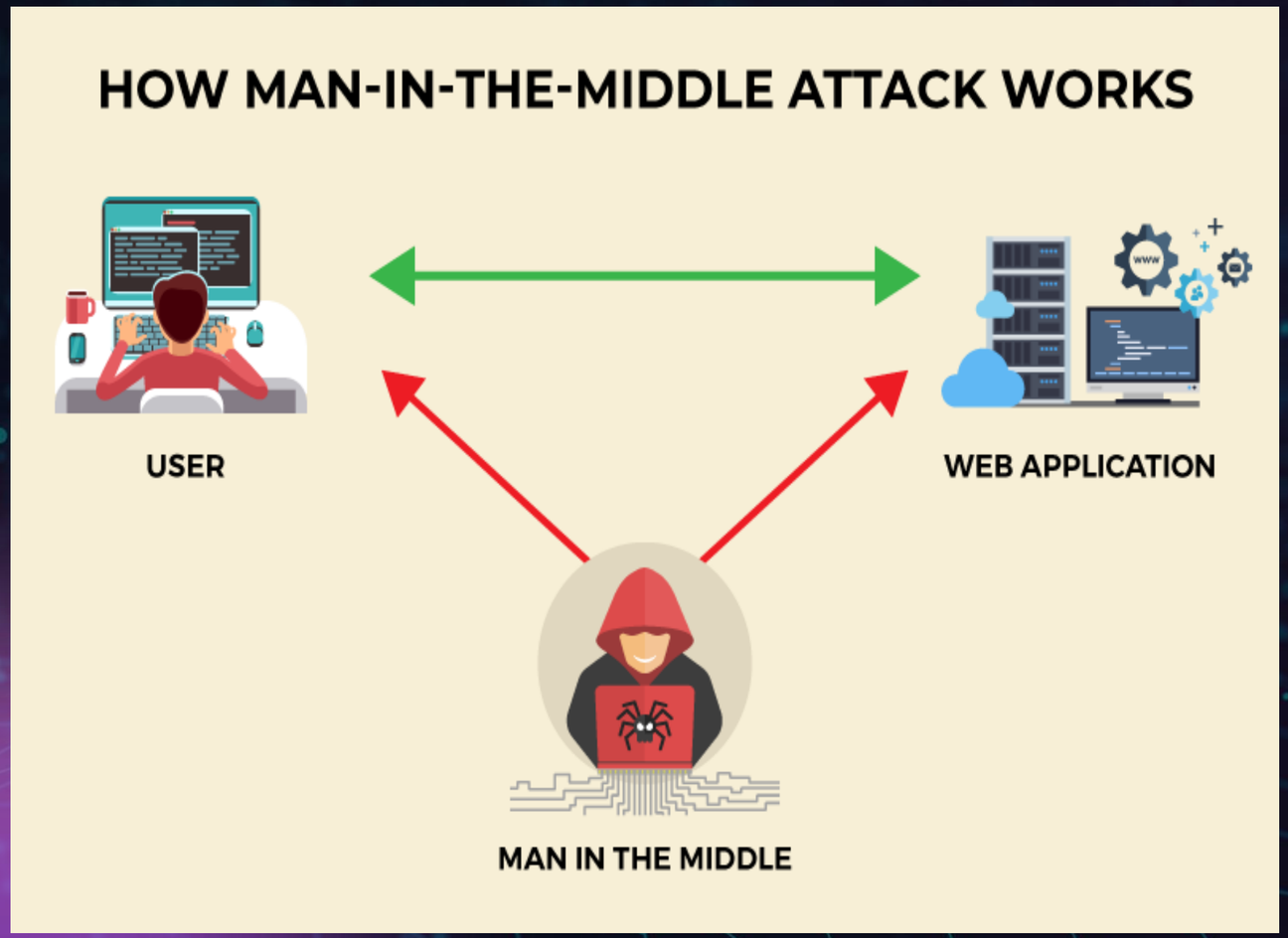


# Rreziqet e përdorimit Wi-Fi publike




| | |
|---|---|
| **Kafene, aeroporte, qytete** | |
| **Jo të sigurta** | Man-in-the-Middle (MITM) attack |
| **Trafik i kapur nga sulmues** | Vjedhje informacioni |
| **“fake hotspot”** | |
| **Jo përdorim account / transaksione sesitive** | Email, banke |
| **Përdorni VPN** | Enkripton trafikun |

# Sulm Man-in-the-Middle (MITM)




Wi-fi publik, router kompromentuar, DNS falsifikuar

Ex: imitim të faqeve web (Web impersonation)

Imitim web legjitime (bankë, email, login etj.)

Sulmuesi: krijon, të lidh me faqe false / klonuar

User komunikon me sulmuesin: fut kredencialet

Sulmuesi: kap të dhënat

User: shpesh më pas ridrejtohet te faqja reale

# Sulm Man-in-the-Middle (MITM)

Shenja imitim Web, rreziku / mbrojtja

Mungon certifikatë sigurie:
HTTPS = HTTP + SSL/TLS

HTTPS false / konfiguruar gabim

Paralajmerim për certifikatën në browser “Ignore warning”

URL me gabime drejtshkrimore

Dalje papritura nga llogaria / ridrejtime

Wi-Fi publik pa fjalëkalim

Mos i injoro paralajmërimet për certifikatën e sigurisë SSL/TLS

Përdor VPN (licensuar) në Wi-Fi public

Kontrollo URL / Domain

Aktivizo MFA

Best: përdor 4G/5G

# Mbrojta ndaj sulmeve kibernetike në jetën personale

01

## Menaxhimi i gjurmës dixhitale

Jo informacionin personal rrjete sociale

02

## Bëja e kopjeve rezervë

Strategjia 3-2-1
3 kopje, 2 media të ndryshme, 1 jashtë lokacionit
Mbrojtje ransomware, dështim pajisje, vjedhje
Testo aftësinë rikuperimit të dhënave

03

## Mbrojtja llogarive online / të dhënave personale

Shkaqe: email e kompromet uar (pikenisje)
Password-e te njejta kudo
Mungesa e MFA (Multi Factor Authentication)
Mosnjohja e politikave te sigurise (ex. banka)

04

## Pasojat reale të një kompromet imi

Akses i paautorizuar në të dhëna
Manipulim te dhenash
Vjedhje/keqpërdorim/shkatërrim te dhënash
Kompromet im personal -> rrezik institucional
(phishing ndaj kolegëve)

# Mbrojta ndaj sulmeve kibernetike në jetën personale

05

## Mbrojta e pajisjeve personale PC, smartphone, router

Ndrysho fjalëkalimet/konfigurimet default (router=admin/admin)

Aktivizo MFA

Kryeni përditësimet e sigurisë/firmware

Jo akses nga interneti (nëse jo e nevojshme)

Perdorni vetëm programe licensuar: OS, Office, antivirus

Backup te te dhenave personale (usb / hard disk te jashtëm / cloud)

Çaktivizo kamer / mikrofon nëse nuk duhet

Shmang aplikacionet e panjohura

Kujdes te shtuar përdorimin Wi-Fi publik (perdor VPN)

Ndani rrjetet

Blini pajisje nga burime certifikuara / serioze

Kontroll prindëror

06

## RAPORTO

Platforma e raportimit të incidenteve për fëmijët dhe qytetarët
https://aksk.gov.al/raporto-5/#

# SIGURIA KIBERNETIKE NË SHTËPINË INTELIGJENTE (SMART HOME)

(+) Komoditet -> (-) Rrezik ?

Router, smartphone / tablet, pc/laptop, TV, kamera, alarm, IoT

Çdo pajisje e lidhur në internet mund të kompromentohet -> fiton akses në gjithe rrjetin shtëpiak

Çdo pajisje lidhur internet potencialisht “portë” hyrje

Smart TV = kompjuter me mikrofon / kamer

IoT përdoret kudo: kamer / alarm / sensor / akses / smart TV, nuk vleresohet si rrezik ?

Shpesh pa konfigurim sigurie

Makina = sistem informatik me rrota (GPS, remote unlocking risks, app mobile, Bluetooth, Wi-Fi)

# Rreziqe Smart Home


Pajisja qëndrore “Router”

“Në botën digjitale, dera e shtëpisë nuk është vetëm çelësi – është edhe Wi-Fi/Router”

Fjalëkalimet e paracaktuar

Mangësi të sigurisë

Aksesi nga interneti të rrjetit shtëpiak

Mbikëqyrja dhe privatësia

# Mbrojtja Smart Home

Siguroni pajisjen “Router:”
kompromet im ruter = rrezik gjithë rrjetin
= shtëpia e ekspozuar

Firewall / Router shtesë më të sofistikuar

Ndryshoni fjalëkalimet e paracaktuar

Zgjedhja / blerja pajisjeve me reputacion

Rishikimi cilësimeve të privatësisë

Përditësoni rregullisht

Izoloni / ndani pajisjet në rrjete të vecanta

Monitoroni aktivitetin

Kufizoni aksesin kamer / mikrofon

# SIGURIA KIBERNETIKE

“Është siguri dhe përgjegjësi e përbashkët

Çdo përdorues (punonjës / qytetar) është pjesë e zinxhirit të sigurisë

Në punë / jetën personale / në shtëpi

Secili prej nesh mund / duhet të bëjë pjesën e vet

Për mbrojtjen e hapësirës digjitale”

# FALEMINDERIT