PËRCEPTIMET SHQIPTARE

PËR KRIMIN KOMPJUTERIK DHE SIGURINË KIBERNETIKE

Abstrakti

Qëllimi i këtij punimi është skanimi, analizimi dhe vlerësimi i perceptimeve të qytetarëve të Republikës së Shqipërisë për krimin dhe sigurinë kibernetike në Shqipëri. Të dhënat që përdoren në këtë punim janë siguruar nëpërmjet anketimit të kryer me pjesëmarrje të gjerë të qytetarëve, të cilët iu përkasin shtresave e profesioneve të ndryshme. Këto të dhëna na informojnë mbi perceptimet e qytetarëve lidhur me rolin dhe ndikimin e teknologjisë së informacionit e komunikimit në raport me shoqërinë e individin; nivelit e njohurive mbi veprat penale në fushën kompjuterike dhe të kërcënimit të krimit kibernetik, nivelin e sigurisë kibernetike si dhe të perceptimeve të tyre rreth legjislacionit e hetimit të këtij krimi si dhe rrugëve të parandalimit të tij. Nëpërmjet analizimit të këtyre perceptimeve synohet evidentimi i problematikave, faktorëve ndikues si dhe dhënia e rekomandimeve për përmirësimin e politikave për parandalimin e reduktimin e tyre, në shërbim të përmirësimit të mëtejshëm të procesit të një policimi bazuar në inteligjencë dhe të sigurisë tonë kombëtare.

Rritja e nivelit të ndërveprimit social dhe tregtar nëpërmjet mjeteve elektronike të komunikimit dhe jo vetëm si dhe tendenca për të orientuar zhvillimin ekonomik drejt teknologjive të avancuara, rrit në mënyrë të pakthyeshme varësinë nga teknologjia e cila, tashmë në terrenin e fituar, kërkon një qasje bashkëpunuese për të arritur shmangien e përdorimit të teknologjisë në kundërshtim me qëllimin kryesor. Por, ashtu siç është e pafund lista e dobishmërive që ofron përdorimi i internetit dhe hapësirës kibernetike, po aq duket se janë dhe prezent rreziqet që kërcënojnë ndërveprimet sociale dhe tregtare.

Interneti i ka dhënë edhe kriminelëve një platformë për t'u rritur dhe përhapur në hapësirën kibernetike. Sot nuk mund të flitet ndaras për krimin kompjuterik apo sigurinë kibernetike, por për individë cybercitizens - qytetarë dixhitalë, edhe familje, shoqëri, organizata, kombe, kriminalitet, kërcënime e siguri, të gjitha së bashku në një hapësirë kibernetike.

Ky zhvillim i vrullshëm i komunikimit masiv në hapësirën kibernetike (virtuale), sidomos pas vitit 2000, po i përball strukturat e Policisë së Shtetit, të agjencive të tjera të zbatimit të ligjit si dhe strukturat e sigurisë me një problematikë të re, në një rritje progresive të veprave penale në fushën kompjuterike, por edhe të kërcënimit kibernetik. Në vendin tonë, në vitin 2017, krahasuar me vitin 2010, janë evidentuar 3.3 herë më shumë vepra penale në fushën e krimeve kompjuterike dhe me një nivel

zbulueshmërie vetëm 27%. Ndërkohë, janë rritur ndjeshëm kërcënimet/sulmet kibernetike, si përpjekje të qëllimshme për të marrë akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë ose disponibilitetin e të dhënave të sistemeve kompjuterike, pa pasur autoritet ligjor për ta bërë këtë.
Në këto kushte, është i domosdoshëm identifikimi i problematikave që lidhen me krimin dhe sigurinë kibernetike, të faktorëve ndikues, të rrugëve për përballimin e tyre me synimin dhënien e rekomandimeve për përmirësimin e politikave për parandalimin dhe reduktimin e krimit kompjuterik e forcimin e sigurisë kibernetike.
Gjatë këtij punimi janë aplikuar metodat dhe instrumentet bazë kërkimore shkencore. Gjetjet e këtij punimi vërtetojnë plotësisht hipotezën tonë se krimi kompjuterik dhe kërcënimi kibernetik vazhdojnë të gjejnë përhapje në Shqipëri ndërmjet të tjerave dhe për shkak të mangësive të theksuara të ndërgjegjësimit/sensibilizimit dhe të edukimit të kategorive shoqërore e shtresave shoqërore me rrezikun e përdorimit të pakontrolluar e të pasigurtë të internetit e të teknologjisë së informacionit e komunikimit. Në përfundim të punimit jepen rekomandimet përkatëse për zhvillimin e politikave për të përmirësuar punën në vazhdim lidhur me mënyrën e trajtimit, menaxhimit, parandalimit dhe reduktimit të krimit e kërcënimit kibernetik në vendin tonë.

Fjale kyçe: Vepra penale ne fushën kompjuterike, krimi kibernetik, internet, anketim, target grup, siguria kibernetike, kërcënimi kibernetik, edukim, trajnim.

Hyrje

Teknologjia e informacionit si një tërësi e teknologjive për mbledhjen, ruajtjen, gjetjen, përpunimin, analizimin, dhe transmetimin e informacionit si dhe interneti, gjithnjë e më tepër po ndërthuret me jetën ekonomike, sociale e politike të individëve, familjeve, organizatave, shteteve e kombeve. Megjithatë, ashtu siç është e pafund lista e shërbimeve që ofron përdorimi i internetit dhe hapësirës kibernetike, po aq duket së janë dhe rreziqet që kërcënojnë këto shërbime nëse keqpërdoret interneti dhe hapësira kibernetike. Keqpërdorimi i internetit dhe hapësirës kibernetike i kthen këto në rreziqe e kërcënime në një "Thembër Akili" për shoqërinë bashkëkohore të informacionit. Interneti ju mundëson edhe kriminelëve një mundësi më shumë për t'u rritur dhe përhapur. Sot nuk mund të flitet ndaras për krimin kompjuterik, kërcënimin kibernetik apo sigurinë kibernetike, por për individ, familje, shoqëri, organizata, kombe, kriminalitet, kërcënime e siguri, të gjitha së bashku në një hapësirë kibernetike. Tashmë edhe njerëzit nuk janë më të zakonshëm si dikur. Ata janë bërë cybercitizens, banorë të hapësirës kibernetike, "qytetarë dixhital" të lidhur më shumë se kurrë më njëri tjetrin.

Për këtë Bashkimi Evropian ka përcaktuar në strategjinë e tij për sigurinë kibernetike se të drejtat themelore, demokracia dhe sundimi i ligjit duhet të mbrohen në hapësirën kibernetike[1].

Zhvillimi i vrullshëm i komunikimit masiv në hapësirën kibernetike (virtuale), sidomos pas vitit 2000, po i përball strukturat e Policisë së Shtetit, të agjencive të tjera të zbatimit të ligjit si dhe strukturat e sigurisë me një problematikë të re, në një rritje progresive të veprave penale në fushën kompjuterike, por edhe të kërcënimit kibernetik. Veprat penale në fushën kompjuterike, janë aktivitete kriminale të zhvilluara në rrjete që kanë si objekt keqpërdorimin e sistemeve dhe të dhënave kompjuterike. Kjo formë e re e veprimtarisë kriminale, e njohur ndërkombëtarisht dhe e pranuar edhe në Shqipëri si krimi kibernetik[2] është e vështirë për t'u hetuar. Në vendin tonë, në vitin 2017, krahasuar me vitin 2010 janë evidentuar 335% më shumë vepra penale në fushën e krimeve kompjuterike dhe janë zbuluar vetëm 27% të autorëve të këtyre veprave penale[3].

Ndërkohë, janë rritur ndjeshëm kërcënimet[4]/sulmet kibernetike, si përpjekje të qëllimshme për të marrë akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë ose disponibilitetin e të dhënave të sistemeve kompjuterike, pa pasur autoritet ligjor për ta bërë këtë[5]. Kriminelët kibernetikë po përdorin metoda gjithnjë e më të sofistikuara për t'u futur në sistemet e informacionit dhe vjedhjen e të dhënave kritike. Rritja e spiunazhi ekonomik dhe aktivitetet e sponsorizuara nga shteti në hapësirën kibernetike përbëjnë një kategori të re të kërcënime për qeveritë dhe kompanitë e BE-së[6].

Në strategjinë tonë të sigurisë kombëtare sulmet kibernetike klasifikohen tashmë në rreziqet e nivelit të parë. Ato kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike[7].

---

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013.

[2] Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, miratuar me VKM Nr. Nr. 973, datë 02.12.2015. Faqe 8.

[3] Informacion përmbledhës i analizave të Sektorit për Hetimin e Krimeve Kompjuterike, për vitet 2016 2018, dinamika e punës, prioritetet, kërkesat".

[4] Kërcënimet mund të kenë origjina të ndryshme, duke përfshirë sulme kriminale, të motivuara politikisht, sulme terroriste apo të sponsorizuar nga shtetet si dhe fatkeqësi natyrore e gabime të paqëllimshme

[5] Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, miratuar me VKM Nr. Nr. 973, datë 02.12.2015. Faqe 7. Burim i cituar.

[6] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013.Burim i cituar.

[7] Strategjia e Sigurisë Kombëtare të Republikës së Shqipërisë, miratuar me Ligjin Nr. 103/2014.

Për identifikimin e problematikave që lidhen me krimin dhe sigurinë kibernetike, të faktorëve ndikues e të rrugëve për përballimin e tyre, përveç të tjerave është e domosdoshme të administrohen dhe analizohen edhe perceptimet e shqiptarëve - cybercitizens rreth këtyre çështjeve. Për këtë arsye është organizuar një anketim i gjerë i kategorive e profesioneve të ndryshme të shoqërisë shqiptare dhe janë analizuar perceptimet e tyre rreth rolit e ndikimit të teknologjisë së informacionit e komunikimit e në raport me shoqërinë e individin; nivelit të njohurive të tyre mbi veprat penale në fushën kompjuterik, të kërcënimit të krimit kibernetik e të nivelit të sigurisë kibernetike si dhe perceptimet e tyre rreth legjislacionin, hetimit dhe rrugëve të parandalimit të këtyre veprave penale dhe jo vetëm. Për më tepër në vijim të punimit.

I. Metodoogjia e anketimit.

I.1. Kampionimi

Nisur nga qëllimi i punimit, për të organizuar një anketim të gjerë u përzgjodhën për të anketuar qytetarë të shtresave e profesioneve dhe konkretisht:

- Gjyqtarë
- Prokurorë
- Kandidatë për magjistrat
- Përfaqësues të biznesit të vogël
- Përfaqësues të biznesit të madh
- Punonjës të sistemit bankar
- Punonjës policie
- Punonjës të Gardës së Republikës
- Studentë
- Nëpunës
- Arsimtarë
- Punëtorë
- Fermerë
- Pension
- Të pa zënë në punë

Të gjithë kategoritë e mësipërme të targetuara u përzgjodhën sepse janë jo vetëm cybercitizens, por dhe aktorë e faktorë në hapësirën kibernetike shqiptare.

I. 2. Përmbajtja e pyetësorit:

Për të gjitha kategoritë u përdor i njëjti model pyetësori. Pyetësori u konceptua dhe u ndërtua me gjashtë pjesë:

- Në pjesën e parë u kërkuan të dhënat demografike të personit që plotëson pyetësorin si mosha, gjinia, arsimi e profesioni.
- Në pjesën e dytë u synua të merret informacion rreth perceptimeve të të anketuarve për teknologjinë e informacionit & komunikimit dhe sigurinë që ofron ajo, raportet e saj me shoqërinë, privatësinë e individit si dhe etikën në komunikimet online.
- Në pjesën e tretë u synua të sigurohet informacioni i nevojshëm për njohuritë e të anketuarit rreth veprave penale në fushën e krimeve kompjuterike si dhe të perceptimeve të tyre rreth aktiviteteve kriminale në fushën kibernetike, pavarësisht nëse ata janë përfitues apo të dëmtuar nga këto aktivitete.
- Në pjesën e katërt u kërkua të merret informacioni i duhur rreth perceptimeve të të anketuarve për gjendjen aktuale të kriminalitetit në fushën kibernetike, formave më të përhapura, gjinisë, moshës, arsimit, shtrirjes gjeografike dhe motiveve që i shtyjnë autorët të përfshihen në krimin kibernetik. Këto të dhëna të grumbulluara, na ndihmojnë të realizojmë një analizë të gjendjes së kriminalitetit në fushën kibernetike nisur nga treguesit subjektivë.
- Në pjesën e pestë u synua të sigurohet informacioni i nevojshëm me perceptimet e të anketuarve rreth nivelit të sigurisë kibernetike dhe shkallës së kërcënimit kibernetik në Shqipëri.
- Në pjesën e gjashtë dhe të fundit u kërkua të sigurohet informacioni i nevojshëm për perceptimet e të anketuarve rreth legjislacionit, hetimi dhe parandalimi të krimit kibernetik.

Pyetjet janë ndërtuar në mënyrë të tillë që të na sigurojnë informacion të krahasueshëm. Pyetësori është tërësisht i standardizuar, me pyetje të mbyllura dhe të orientuara në përgjigje. Alternativat e përgjigjeve janë të vendosura në formë matrice, në trajtën e shkallëve të rëndësisë (1, 2, 3, 4, 5).[8]

Nga pyetësori i standardizuar ne arritëm të sigurojmë nga burime parësore informacion të krahasueshëm. Ky informacion i grumbulluar na mundësoi të bëjmë analiza të kryqëzuara të të dhënave të cilat ndikuan ndjeshëm në gjetjet interesante të këtij punimi si dhe në hartimin e rekomandimeve rreth krimit kompjuterik e sigurisë kibernetike në Shqipëri.

I.3. Mënyra e shpërndarjes dhe plotësimit të pyetësorit:

Për herë të parë ne organizuam anketimin online me programin "Enalyzer", duke ju dhënë mundësi pjesëtarëve të grupeve të përzgjedhura, që sipas dëshirës së tyre të

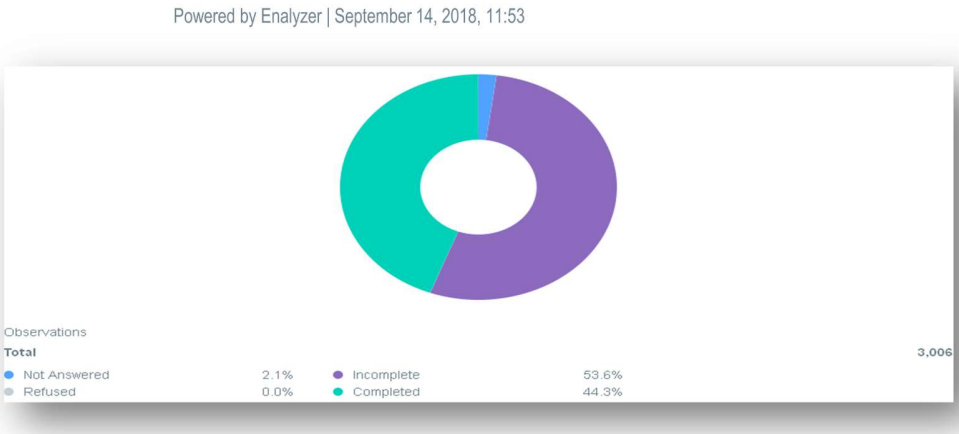
[8] Sipas nivelit i korrespondon: shkalla 1 – aspak ; shkalla 2 – pak; shkalla 3 – disi; shkalla 4 – mjaftueshëm dhe shkalla 5 – shumë. Të anketuarit zgjedhin gjithmonë një shkallë vlerësimi për çdo kategori apo nënkategori, sipas pyetjeve të pyetësorit.

merrnin pjesë në këtë anketim, duke plotësuar on line nga kompjuteri apo smartfoni i tyre, në linkun https://surveys.enalyzer.com/?pid=f2q2s5r7, pyetësorin e përgatitur nga ana jonë.

I.4. Realizimi i procesit të anketimit:

Procesi i anketimit u zhvillua në një hark kohor prej 7 ditësh. Deri më datën 14 Shtator 2018, në ora 11.53, në anketim kanë marrë pjesë 3006 persona. Nga këta 44.3% (1334 persona) e kanë përfunduar plotësisht anketimin, 53.6% (1611 persona) nuk e kanë përfunduar plotësisht anketimin ndërsa 2.1% nuk e kanë plotësuar atë (Grafiku 1).
Në analizën tonë, shifra prej 53.6% e pjesëmarrësve që nuk e kanë përfunduar plotësisht anketimin lidhet si me mungesën e një përgjegjshmërive sociale të një pjesë jo të vogël të pjesëtarëve të target grupeve të përzgjedhura për të marrë pjesë në anketime të tilla për probleme kaq të rëndësishme për shoqërinë shqiptare po aq dhe me mungesën e eksperiencës së tyre në anketimet online apo dhe për arsye teknike, pasi nuk kanë klikuar në fund të procesit të plotësimit të pyetësorin në "End Survey".

Grafiku 1



Për interesa të këtij studimi, ne do të përpunojmë dhe analizojmë treguesit dhe përgjigjet e atyre pjesëmarrësve në anketim që e kanë kompletuar intervistën nga pyetja e parë deri tek e fundit. Këta përbëjnë 44.3% të pjesëmarrësve ose gjithsej 1334 persona. Ky kampion përmbush plotësisht standardet ndërkombëtare të një anketimi profesional.

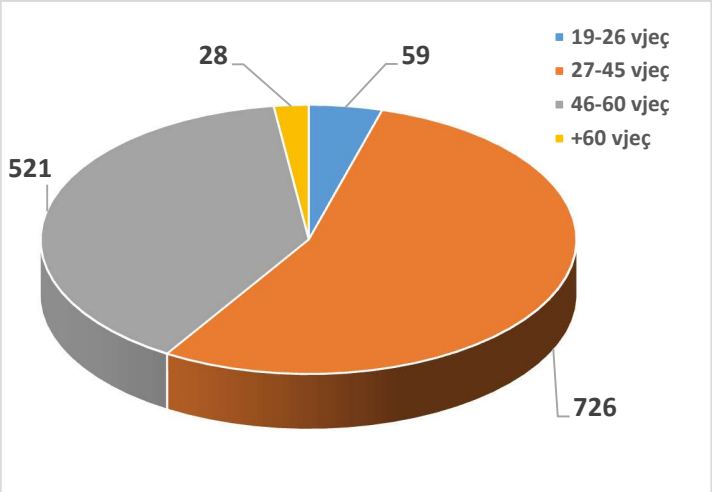
II. Përbërja e kampionimit sipas grupmoshës, gjinisë, arsimit e profesionit.

Në pjesën e parë të pyetësorit janë përfituar të dhënat rreth grupmoshës, gjinisë, arsimit e profesionit si më poshtë:

❖ **Grupmosha e kampionimit:**

Të anketuarit sipas grupmoshave në paraqitje tabelore dhe grafike janë si më poshtë**:**

GRUPMOSHA			
		Frekuenca	Përqindja
Të Vlefshme	19-26 vjeç	59	4.4
	27-45 vjeç	726	54.4
	46-60 vjeç	521	39.1
	+60 vjeç	28	2.1
	Total	1334	100.0

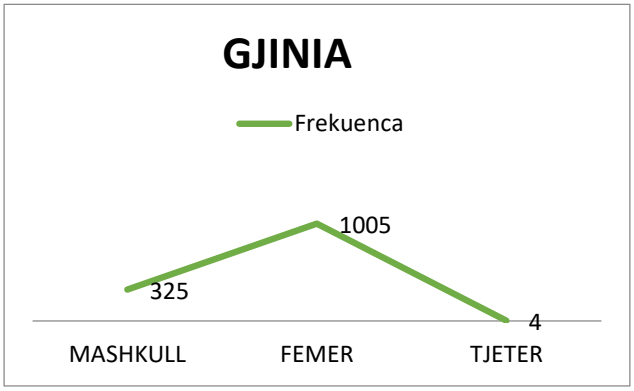


Nga analiza krahasimore e gjetjeve të mësipërme mund të konkludojmë se, në anketim kanë marrë pjesë nga të gjithë grupmoshat të cilave iu është adresuar pyetësori. Më shumë e përfaqësuar është grupmosha 27-45 vjeç dhe 46-60 vjeç. Duket këto dy grupmosha kanë pasur më shumë interes për fushën e krimeve dhe sigurisë kibernetike. Më pak të përfaqësuara janë grupmoshat mbi 60 vjeç dhe 19-26 vjeç.

- **Gjinia e kampionimit.**

Të anketuarit sipas gjinisë, në paraqitje tabelore dhe grafike janë si më poshtë:

GJINIA			
		Frekuenca	Përqindja
Të Vlefshme	MASHKULL	325	24.4
	FEMER	1005	75.3
	TJETER	4	.3
	Total	1334	100.0

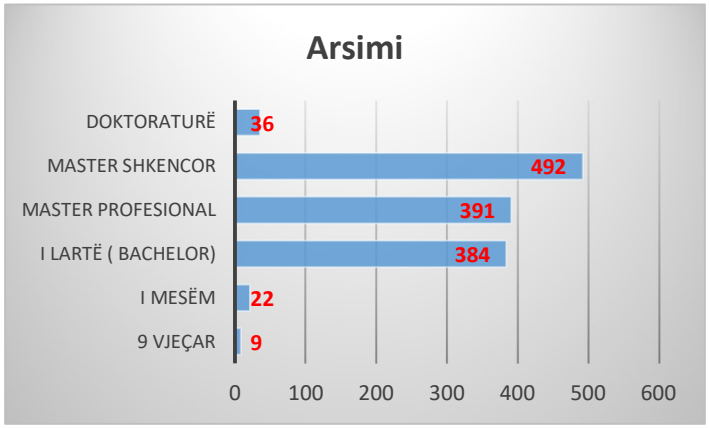


Nga kjo mund të konkludojmë se të anketuarit femrat kanë qenë më të interesuara dhe më të ndjeshme për tematikën e anketimit, me një përgjegjshmëri më të madhe sociale se meshkujt si dhe më të sakta në plotësimin e pyetësorit nga fillimi në fund.

- **Niveli arsimor i kampionimit.**

Niveli arsimor i të anketuarve, në paraqitje tabelore dhe grafike është si më poshtë:

ARSIMI			
		Frekuenca	%
Të Vlefshme	9 vjeçar	9	0.7
	I Mesëm	22	1.6
	I lartë (Bachelor)	384	28.8
	Master Profesional	391	29.3
	Master Shkencor	492	36.9
	Doktoraturë	36	2.7
	Total	1334	100.0

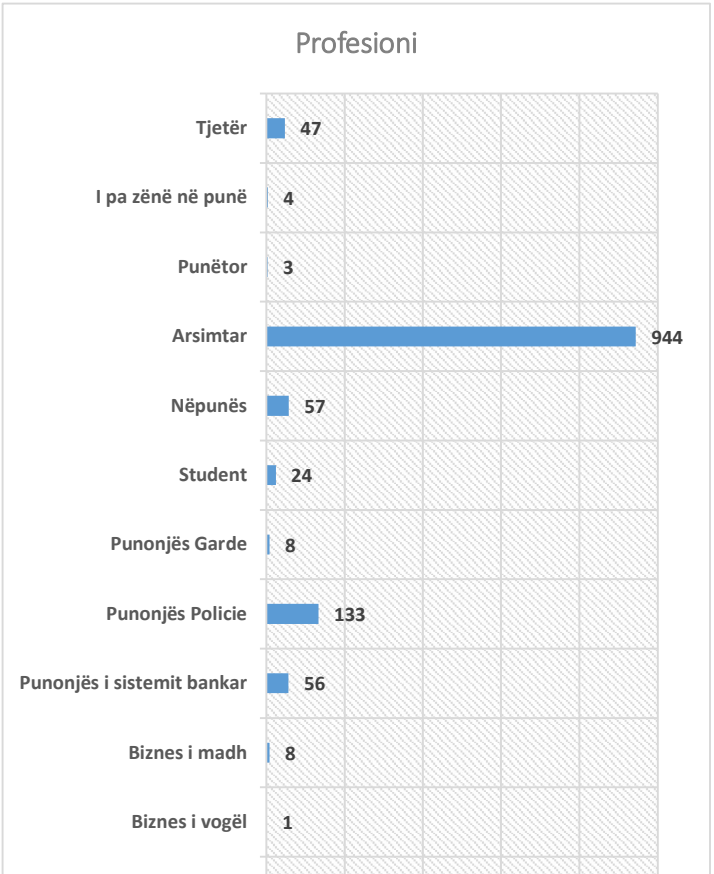


Nga analiza krahasimore e të dhënave të mësipërme, mund të konkludojmë se 97.7% e kampionimit ka një nivel të lartë arsimor (bachelor, master dhe doktoraturë). Kjo na bën optimist në cilësinë e përgjigjeve të tyre, por njëkohësisht na obligon që në të ardhmen të organizojmë një anketim tjetër në mënyrë që të njohim dhe perceptimet dhe shkallën e njohurive për krimin kibernetik të grupmoshave nën 26 vjeç, të cilat janë shumë aktive në përdorimin e internetit dhe të teknologjisë së informacionit.

- **Kampionimi sipas përbërjes profesionale.**

Të anketuarit sipas profesionit, në paraqitje tabelore dhe grafike janë si më poshtë:

Profesioni			
		Frekuenca	%
Të Vlefshme	Gjyqtar	16	1.2
	Prokuror	10	0.7
	Kandidat për Magjistrat	23	1.7
	Biznes i vogël	1	0.1
	Biznes i madh	8	0.6
	Punonjës i sistemit bankar	56	4.2
	Punonjës Policie	133	10.0



	Punonjës Garde	8	0.6
	Student	24	1.8
	Nëpunës	57	4.3
	Arsimtar	944	70.8
	Punëtor	3	0.2
	I pa zënë në punë	4	0.3
	Tjetër	47	3.5
	Total	1334	100.0

Nga analiza krahasimore e gjetjeve të mësipërme të përbërjes profesionale të kampionimit mund të konkludojmë se ai ka një përfaqësim e larmishmëri ku numrin më të madh e përbëjnë arsimtarët (70.8%) dhe punonjësit e policisë (10%) ndërsa më pak nga bota e biznesit dhe punëtorët. Kategoritë që përfaqësohen në këtë kampionim jo vetëm janë vetë përdorues të internetit dhe teknologjisë së informacionit, por janë dhe aktorë në luftën kundër krimit kibernetik (gjyqtarët, prokurorët, punonjësit e policisë dhe arsimtarët). Gjithashtu mund konkludojmë se arsimtarët, në raport me gjyqtarët, prokurorët dhe punonjësit e policisë, tregojnë një nivel përgjegjshmëri më të madhe sociale, duke u angazhuar në anketime në probleme kaq të rëndësishme për shoqërinë shqiptare, siç është krimi kompjuterik dhe siguria kibernetike.

III. Gjetjet e procesit të anketimit dhe analizimi i tyre.

Në këtë punim, për shkak dhe të hapësirës në dispozicion, ne do të analizojmë një pjesë të të dhënave të këtij anketimi e kryesisht ato që lidhen me perceptimet për sigurinë kibernetike.

Sipas Strategjisë së Bashkimit Evropian për Sigurinë Kibernetike, për një hapësirë kibernetike të hapur, të sigurt dhe të mbrojtur, siguria kibernetike përpiqet të ruajë disponueshmërinë dhe integritetin e rrjeteve dhe infrastrukturës, si dhe fshehtësinë e informatave që mbahen në to [9]. Ndërsa, Organizata Ndërkombëtare e Standardizimit (ISO) përkufizon sigurinë kibernetike si "ruajtje të konfidencialitetit, integritetit dhe disponueshmërisë së informatave në hapësirën kibernetike". Definicionet e tjera e definojnë sigurinë kibernetike si objektiv të dëshiruar të fushës së sigurisë së TI-së, në të

[9] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. faqe 3. Shfletuar me 28.10.2018.

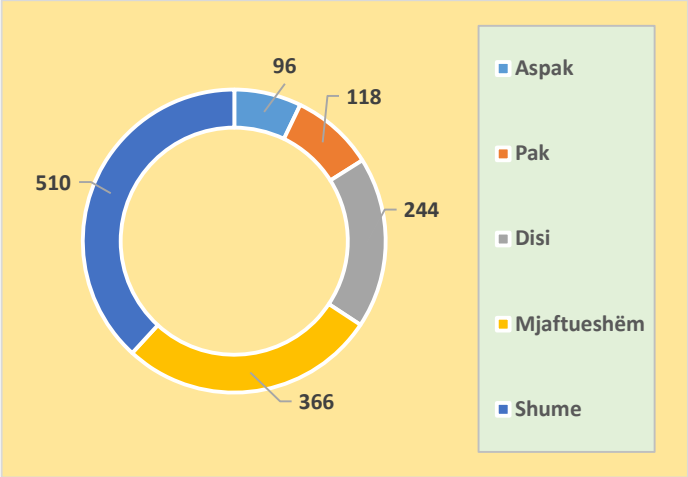
cilën rreziqet e hapësirës globale kibernetike ngushtohen deri në një minimum të pranueshëm[10].

Gjetjet lidhur me perceptimet e të anketuarve për sigurinë kibernetike sipas pyetjeve të adresuara janë si më poshtë:

- Përgjigjet e të anketuarve për pyetjen se sa ndikon zhvillimi i teknologjisë së informacionit dhe komunikimit në fushën e privatësisë, më paraqitje tabelore dhe grafike janë si më poshtë:

Sipas jush, sa ndikon zhvillimi i teknologjisë së informacionit dhe komunikimit në fushën e privatësisë

		Frekuenca	%
Të Vlefshme	Aspak	96	7.2
	Pak	118	8.8
	Disi	244	18.3
	Mjaftueshëm	366	27.4
	Shume	510	38.2
	Total	1334	100.0



Nga studimi i përgjigjeve të anketuarve për pyetjen se sa ndikon zhvillimi i teknologjisë së informacionit dhe komunikimit në fushën e privatësisë gjejmë se, për të anketuarit ky zhvillim ndikon disi, mjaftueshëm dhe shumë në fushën e privatësisë në masën 18.3%, 27.4% dhe 38.2%.

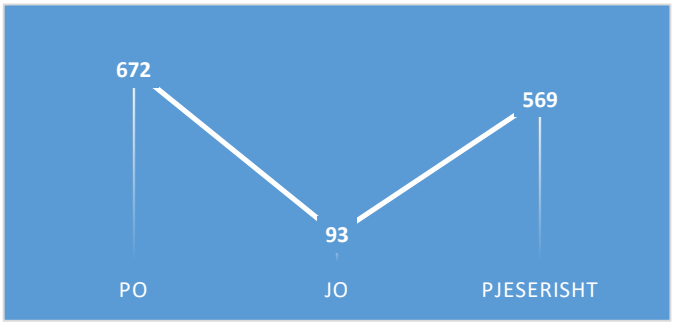
Nga analiza e gjetjeve të mësipërme mund të konkludojmë se për 83.9% të të anektuarve zhvillimi i teknologjisë së informacionit dhe komunikimit ndikon disi, mjaftueshëm dhe shumë në fushën e privatësisë.

- **Përgjigjet e të anketuarve për pyetjen nëse e cenon zhvillimi i teknologjisë së informacionit dhe komunikimit privatësinë, në paraqitje tabelore dhe grafike janë si më poshtë:**

[10] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019. Republika e Kosovës, Qeveria e Kosovës, Ministria e Punëve të Brendshme. Dhjetor 2015. Faqe 7.

A e cenon privatësinë zhvillimi i teknologjisë së informacionit & komunikimit

		Frekuenca	%
Të Vlefshme	PO	672	50.4
	JO	93	7.0
	PJESERISHT	569	42.7
	Total	1334	100.0



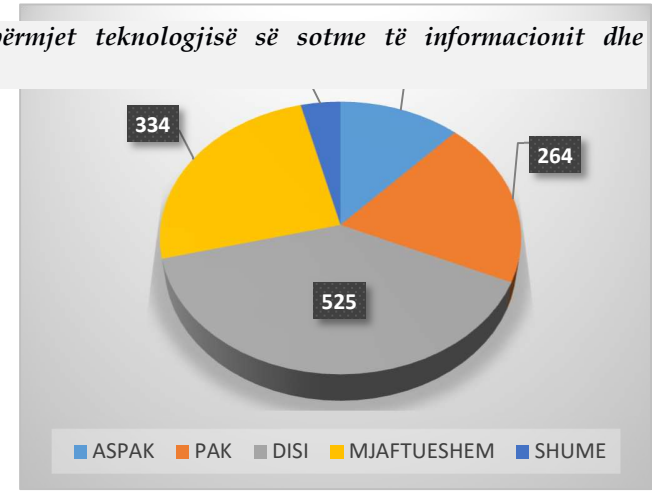
Nga studimi i përgjigjeve të anketuarve për pyetjen se nëse e cenon zhvillimi i teknologjisë së informacionit dhe komunikimit privatësinë gjejmë se, 50.4% e tyre mendojnë se zhvillimi i teknologjisë së informacionit dhe komunikimit cenon privatësinë; 42.7 % e cenon "pjesërisht" dhe vetëm 7% mendojnë se ky zhvillim teknologjik nuk e cenon privatësinë.

Nga analiza e gjetjeve të mësipërme mund të konkludojmë se, për 93 % të të anketuarve zhvillimi i teknologjisë së informacionit dhe komunikimit cenon privatësinë qoftë dhe pjesërisht, shifër kjo shumë e lartë.

- **Përgjigjet e të anketuarve për pyetjen se sa të sigurt e konsiderojnë komunikimin nëpërmjet teknologjisë së sotme të informacioni dhe komunikimit në paraqitje tabelore dhe grafike është si më poshtë:**

Sa të sigurt e konsideroni komunikimin nëpërmjet teknologjisë së sotme të informacionit dhe komunikimit?

		Frekuenca	%
Të Vlefshme	ASPAK	159	11.9
	PAK	264	19.8
	DISI	525	39.4
	MJAFTUESHEM	334	25.0
	SHUME	52	3.9
	Total	1334	100.0



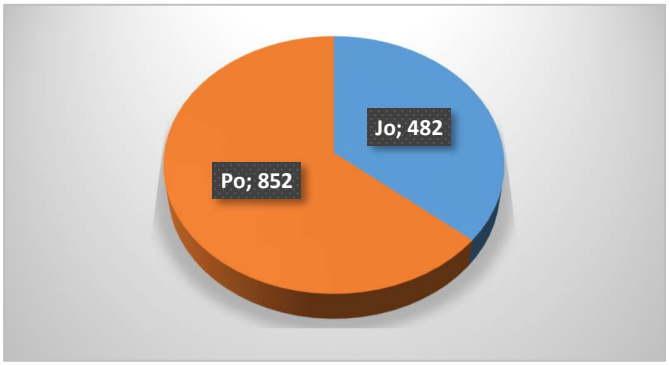
Nga studimi i përgjigjeve të anketuarve për pyetjen se sa të sigurt e konsiderojnë komunikimin nëpërmjet teknologjisë së sotme të informacioni dhe komunikimit gjejmë se 11.9% e të anketuarve nuk ndjehen "aspak" të sigurt në komunikimin nëpërmjet teknologjisë së sotme të informacioni dhe komunikimit. Ndërkohë që 19.8% ndjehen "pak", 39.4% ndjehen "disi", 25% ndjehen mjaftueshëm dhe vetëm 3.9% ndjehen "shumë" të sigurtë në komunikimet nëpërmjet kësaj teknologjie.

Në përfundim të analizës së të dhënave statistikore (tabelore dhe grafike) të kësaj pjese të përgjigjeve të të anketuarve mund të konkludojmë se, shumica e të anketuarve mendojnë se zhvillimi i teknologjisë së sotme të informacionit dhe komunikimit luan rol të rëndësishëm në të gjithë aspektet e jetës duke përfshirë biznesin, komunikimin dhe edukimin, aksesin në informacion e shërbime publike dhe në fushën e privatësisë. Për shumicën e të anketuarve ky zhvillim teknologjik, cenon privatësinë. Për 31.7% të tyre ky komunikim nuk është aspak i sigurt ose është pak i sigurt.

Format kryesore nga të cilat të anketuarit e ndjejnë veten më të kërcënuar janë si më poshtë:

- Nga sulmet me viruse e ndjejnë veten të cenuar 63.9% e të anketuarve.

A e keni ndjerë veten të cënuar nga sulmi me viruse			
		Frekuenca	%
Të Vlefshme	Jo	482	36.1
	Po	852	63.9
	Total	1334	100.0



A e keni ndjerë veten të cënuar nga mashtrime kompjuterike (online)			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1129	84.6
	Po	205	15.4
	Total	1334	100.0

- Nga mashtrimi kompjuterik e ndjejnë veten të cenuar 15.4% e të anketuarve

Vlefshme	Po	185	13.9
	Total	1334	100.0

A keni ndjerë veten të cënuar nga hyrja e pa autorizuar kompjuterike			
		Frekuenca	Përqindja
Të	Jo	1149	86.1

- Nga hyrja e paautorizuar në kompjuter e ndjejnë veten të cenuar 13.9% e të anketuarve

A keni ndjerë veten të cënuar nga ndërhyrja në të dhënat kompjuterike			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1178	88.3
	Po	156	11.7
	Total	1334	100.0

- Nga ndërhyrja në të dhënat kompjuterike e ndjejnë veten të cenuar 11.7% e të anketuarve.

A keni ndjerë veten të cënuar nga përgjim të paligjshëm			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1153	86.4
	Po	181	13.6
	Total	1334	100.0

- Nga përgjimet e paligjshme e ndjejnë veten të cenuar 11.7% e të anketuarve

A keni ndjerë veten të cënuar nga vjedhja e identitetit			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1123	84.2
	Po	211	15.8
	Total	1334	100.0

- Nga vjedhja e identitetit e ndjejnë veten të cenuar 15.8% e të anketuarve.

A keni ndjerë veten të cënuar nga shkelje e te drejtës së autorit dhe pronësisë industriale			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1222	91.6
	Po	112	8.4
	Total	1334	100.0

- Nga shkelje e te drejtës së autorit dhe pronësisë industriale e ndjejnë veten të cenuar 8.4% e të anketuarve.

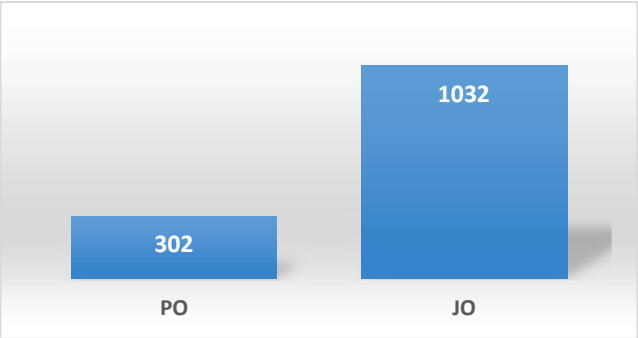
A keni ndjerë veten të cënuar nga forma te tjera të ndërhyrjes kompjuterike			
		Frekuenca	Përqindja
Të Vlefshme	Jo	998	74.8
	Po	336	25.2
	Total	1334	100.0

- Nga forma të tjera, të pa listuara më lart, e ndjejnë veten të cenuar 25.2% e të anketuarve.

Nga analiza e gjetjeve të mësipërme mund të konkludojmë se të anketuarit e ndjejnë vetëm më shumë të kërcënuar nga sulmet me viruse, vjedhjet e identitetit dhe mashtrimet kompjuterike.

- **Përgjigjet e të anketuarve lidhur me pyetjen nëse kanë përjetuar ndonjëherë pasoja të krimeve kibernetike, në paraqitje tabelore dhe grafike është si më poshtë**:

A keni përjetuar ndonjëherë pasoja të krimeve kibernetike?			
		Frekuenca	%
Të Vlefshme	PO	302	22.6
	JO	1032	77.4
	Total	1334	100.0



Nga analiza e përgjigjeve të mësipërme gjejmë se 22.6% e të anketuarve kanë përjetuar pasoja të krimeve kibernetike, shifër kjo relativisht e lartë.

a. Llojet e pasojave të krimeve kibernetike që kanë përjetuar të anketuarit paraqiten si më poshtë:

A keni përjetuar ndonjëherë pasoja financiare nga krimet kibernetike?			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1270	95.2
	Po	64	4.8
	Total	1334	100.0

☞ Nga krimet kibernetike kanë përjetuar pasoja financiare 4.8% e të anketuarve.

A keni përjetuar ndonjëherë humbjen e të dhënave kompjuterike si pasoja të krimeve kibernetike?			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1019	76.4
	Po	315	23.6
	Total	1334	100.0

☞ Humbje të të dhënave kompjuterike si pasojë e krimeve kibernetike kanë përjetuar 23.6% e të anketuarve.

A keni përjetuar ndonjëherë vjedhje të identitetit online si pasoje e krimeve kibernetike			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1094	82.0
	Po	240	18.0
	Total	1334	100.0

☞ Vjedhje të identitetit online kanë përjetuar 18% e të anketuarve

A keni përjetuar ndonjëherë pasoja të tjera pervec sa me siper nga krimet kibernetike?			
		Frekuenca	Përqindja
Të Vlefshme	Jo	535	40.1
	Po	799	59.9
	Total	1334	100.0

☞ Pasoja të tjera nga krimet kibernetike, përveç listimit të

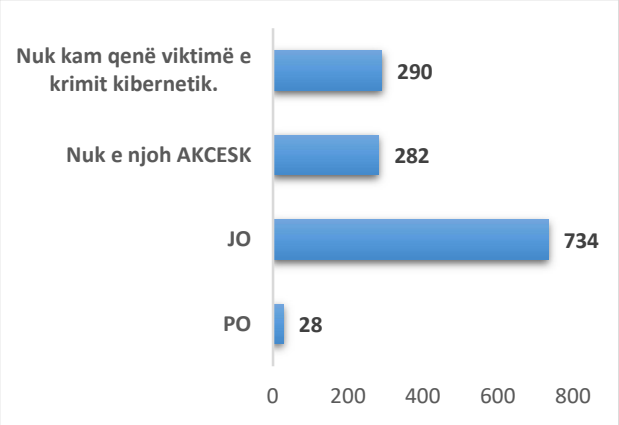
mësipërm, kanë përjetuar 59.9% e . të anketuarve

Nga analiza e gjetjeve të të mësipërme mund të konkludojmë se 22.6%e të anketuarve kanë qenë të paktën një herë viktimë e krimit kibernetik, ndërkohë që pasojat kanë qenë më shumë në formën e humbjes së të dhënave kompjuterike (23.6%), vjedhje të identitetit (18%) si dhe forma të tjera të pasojave (59.9%) .

- **Përgjigjet e të anketuarve lidhur me pyetjen nëse kanë** raportuar apo kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK), në paraqitje tabelore dhe grafike janë si më poshtë:

A keni raportuar dhe kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK)?

A keni raportuar dhe kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK)?			
		Frekuenca	%
Të Vlefshme	PO	28	2.1
	JO	734	55.0
	NUK E NJOH AKCESK	282	21.1
	Nuk kam qenë viktimë e krimit kibernetik.	290	21.7
	Total	1334	100.0

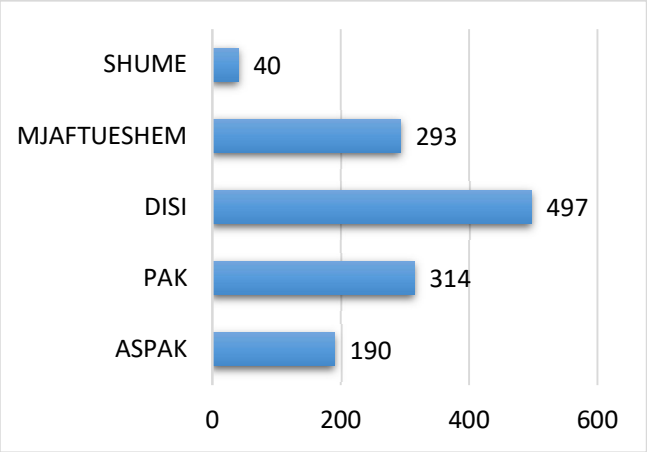


Nga analiza e gjetjeve të mësipërme konkludojmë se të anketuarit nuk kanë kërkuar asistencë pranë autoritetit kryesor kombëtar të sigurisë kibernetike në rastet e përjetimit të pasojave nga krimet kibernetike. Gjithashtu, konsiderohet jo i vogël edhe numri i të anketuarve që nuk e njohin fare atë institucion.

- **Përgjigjet e të anketuarve për pyetjen se sa të sigurt ndjehen ata në aktivitetet specifike në hapësirën kibernetike**, në paraqitje tabelore dhe grafike janë si më poshtë. Nga kjo paraqitje gjejmë se:
- **Në aktivitetet online në rrjetet sociale**, të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht me 37.3%, 22% dhe 3%.

Sa të sigurt ndjeheni në aktivitetet online në rrjetet sociale?

		Frekuenca	%
Të Vlefshme	ASPAK	190	14.2
	PAK	314	23.5
	DISI	497	37.3
	MJAFTUESHEM	293	22.0
	SHUME	40	3.0
	Total	1334	100.0

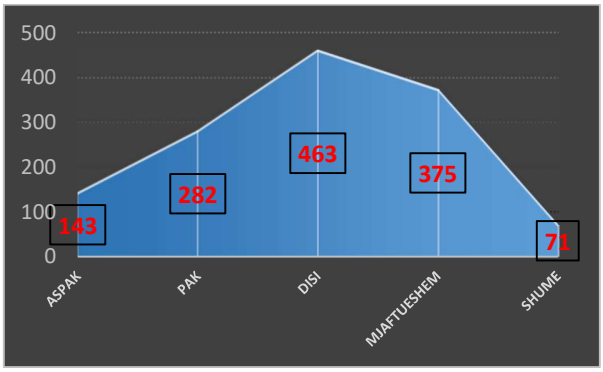


☞ **Në postën elektronike**, të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht me 32.6%, 34.3% dhe 6.4%.

Sa të sigurt ndjeheni në aktivitetin tuaj me postën elektronike?			
		Frekuenca	Përqindja
Të Vlefshme	ASPAK	110	8.2
	PAK	245	18.4
	DISI	435	32.6
	MJAFTUESHEM	458	34.3
	SHUME	86	6.4
	Total	1334	100.0

☞ **Në komunikimin online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 34.7%, 28.1% dhe 5.3%;**

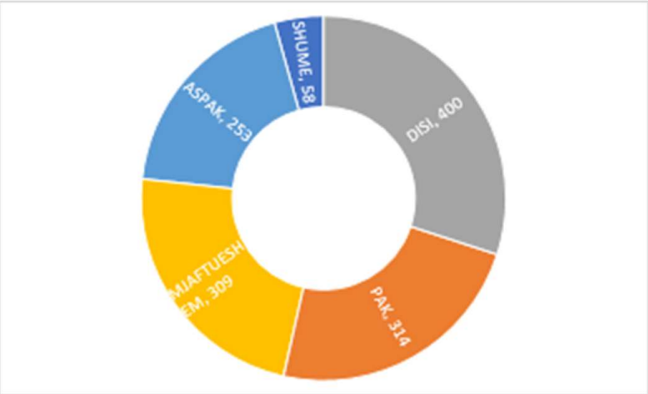
Sa të sigurt ndjeheni në komunikimin online?			
		Frekuenca	%
Të Vlefshme	ASPAK	143	10.7
	PAK	282	21.1
	DISI	463	34.7
	MJAFTUESHEM	375	28.1
	SHUME	71	5.3
	Total	1334	100.0



☞ **Në blerjet online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 30%, 23.2% dhe 4.3%.**

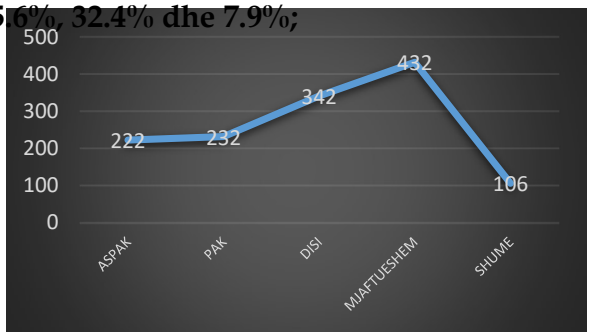
Sa të sigurt ndjeheni

në blerjet online?			
		Frekuenca	%
Të Vlefshme	ASPAK	253	19.0
	PAK	314	23.5
	DISI	400	30.0
	MJAFTUESHEM	309	23.2
	SHUME	58	4.3
	Total	1334	100.0



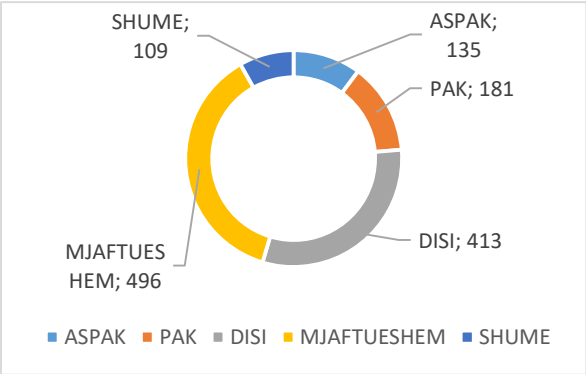
- **Në veprimet bankare online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 25.6%, 32.4% dhe 7.9%;**

Sa të sigurt ndjeheni në veprimet bankare onlinë			
		Frekuenca	%
Të Vlefshme	ASPAK	222	16.6
	PAK	232	17.4
	DISI	342	25.6
	MJAFTUESHEM	432	32.4
	SHUME	106	7.9
	Total	1334	100.0



- **Gjatë punës në kompjuterin në zyrë të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 31%, 37.2% dhe 8.2%.**

Sa të sigurt ndjeheni gjatë punës në kompjuterin në zyrë?			
		Frekuenca	%
Të Vlefshme	ASPAK	135	10.1
	PAK	181	13.6
	DISI	413	31.0
	MJAFTUESHEM	496	37.2
	SHUME	109	8.2
	Total	1334	100.0



- Gjatë punës me kompjuterin në shtëpi të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht me 32.5%, 38.1% dhe 8.2%;

Sa të sigurt ndjeheni gjatë punës në kompjuterin në shtëpi

		Frekuenca	Përqindja
Të Vlefshme	ASPAK	93	7.0
	PAK	189	14.2
	DISI	434	32.5
	MJAFTUESHEM	508	38.1
	SHUME	110	8.2
	Total	1334	100.0

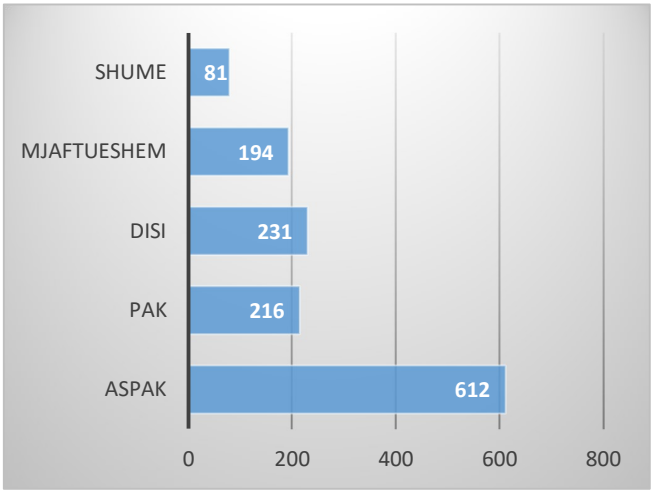
- Në shkeljen e etikës në komunikim online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht 34.4%, 36.7% dhe 10%;

Sa të sigurt ndjeheni nga shkelja e etikës në komunikim online në hapësirën kibernetike?

		Frekuenca	Përqindja
Të Vlefshme	ASPAK	73	5.5
	PAK	178	13.3
	DISI	459	34.4
	MJAFTUESHEM	490	36.7
	SHUME	134	10.0
	Total	1334	100.0

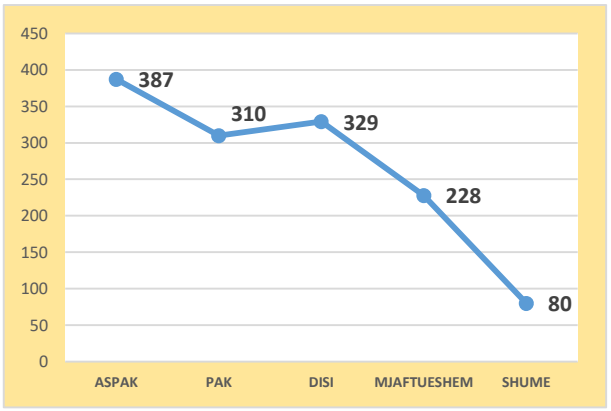
☞ Gjatë ndarjes së pasëordit (fjalëkalimit) me të tjerët të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 17.3%; 14.5% dhe 6.1%;

Sa të sigurt ndjeheni gjatë ndarjes së pasëordit (fjalëkalimit) me të tjerët			
		Frekuenca	%
Të Vlefshme	ASPAK	612	45.9
	PAK	216	16.2
	DISI	231	17.3
	MJAFTUESHEM	194	14.5
	SHUME	81	6.1
	Total	1334	100.0



☞ Në përdorimin vetëm të një pasëordi në të gjitha shërbimet online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht me 24.7%,17.1% dhe 6%;

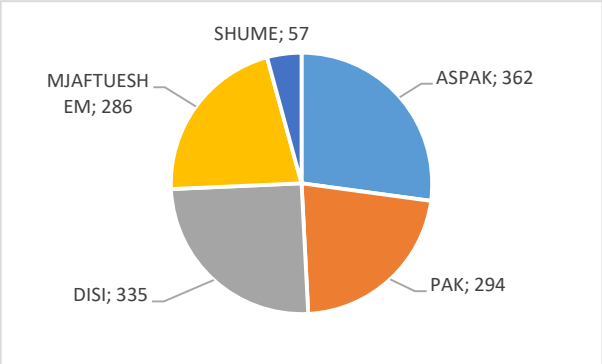
Sa të sigurt ndjeheni në përdorimin e vetëm të një pasëordi në të gjitha shërbimet online.			
		Frekuenca	%
Të Vlefshme	ASPAK	387	29.0
	PAK	310	23.2
	DISI	329	24.7
	MJAFTUESHEM	228	17.1
	SHUME	80	6.0
	Total	1334	100.0



☞ Në përdorimin e kartave të kreditit online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht me 25.1%,21.4% dhe 4.3%;

Sa të sigurt ndjeheni në secilin prej aktiviteteve dhe veprimeve të mëposhtme në hapësirën kibernetike? *Përdorimi i kartave të kreditit online*		
	Frekuenc	%

		a	
Të Vlefshme	ASPAK	362	27.1
	PAK	294	22.0
	DISI	335	25.1
	MJAFTUESHEM	286	21.4
	SHUME	57	4.3
	Total	1334	100.0



☞ Në përdorimin e shërbimeve publike online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurtë përkatësisht me 34.2%, 26.9% dhe 4.5%

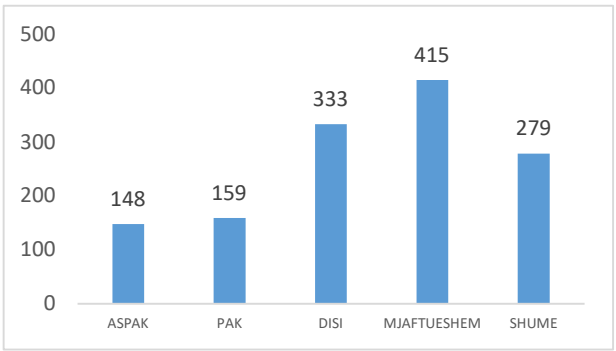
Sa të sigurt ndjeheni në përdorimin e shërbimeve publike online			
		Frekuenca	Përqindja
Të Vlefshme	ASPAK	176	13.2
	PAK	283	21.2
	DISI	456	34.2
	MJAFTUESHEM	359	26.9
	SHUME	60	4.5
	Total	1334	100.0

Nga analiza e gjetjeve të përgjigjeve të anketuarve për pyetjen se sa të sigurt ndjehen ata në aktivitetet e tyre specifike në hapësirën kibernetike mund të konkludojmë se të anketuarit nuk ndjehen të sigurt në aktivitetet e tyre në hapësirën kibernetike në masën nga 18.8% deri në 62.1%.

Konkretisht ndjehen në masën 37.7% "aspak" dhe "pak" të sigurt në aktivitetet online në rrjetet sociale; 26.6% në postën elektronike; 31.8% në komunikimin online; 42.5% në blerjet online; 34% në veprimet bankare; 23.7% gjatë punës me kompjuter në zyrë; 21.2% gjatë punës me kompjuterin në shtëpi; 18.8% në shkeljen e etikës në komunikim online; 62.1% gjatë ndarjes së pasëordit (fjalëkalimit) me të tjerët; 52.2% në përdorimi vetëm të një pasëordi në të gjitha shërbimet online; 47.1% në përdorimin e kartave të kreditit online dhe 34.4% në përdorimin e shërbimeve publike online.

- **Përgjigjet e të anketuarve për pyetjen se a ndjeni përgjegjësi për sigurinë kibernetike në vendin e tuaj të punës, në paraqitje tabelore dhe grafike janë si më poshtë:**

A ndjeni përgjegjësi për sigurinë kibernetike në vendin tuaj të punës?			
		Frekuenca	%
Të Vlefshme	ASPAK	148	11.1
	PAK	159	11.9
	DISI	333	25.0
	MJAFTUESHEM	415	31.1

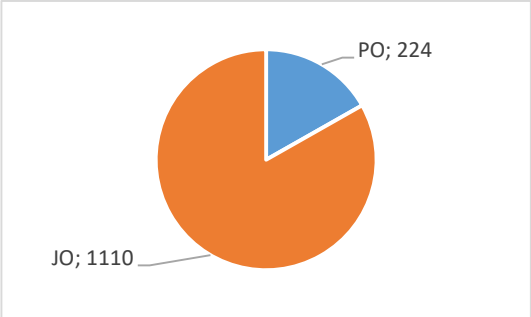


	SHUME	279	20.9
	Total	1334	100.0

Nga analiza e gjetjeve të mësipërme mund të konkludojmë se të anketuarit që nuk ndjejnë "aspak" përgjegjësi apo që ndjejnë "pak" dhe "disi" përgjegjësi për sigurinë kibernetike në vendin e tyre të punës përbëjnë 47 % të numrit total të intervistuarve shifër kjo mjaft e lartë. Kjo na obligon për rritjen e përgjegjshmërisë për sigurinë kibernetike të punonjësve në qendrën e tyre të punës.

- **Përgjigjet e të anketuarve për pyetjen nëse janë trajnuar për sigurinë kibernetike në vendin e tuaj të punës, në paraqitje tabelore dhe grafike janë si më poshtë**.

A jeni i trajnuar për sigurinë kibernetike në vendin tuaj të punës?			
		Frekuenca	%
Të Vlefshme	PO	224	16.8
	JO	1110	83.2
	Total	1334	100.0

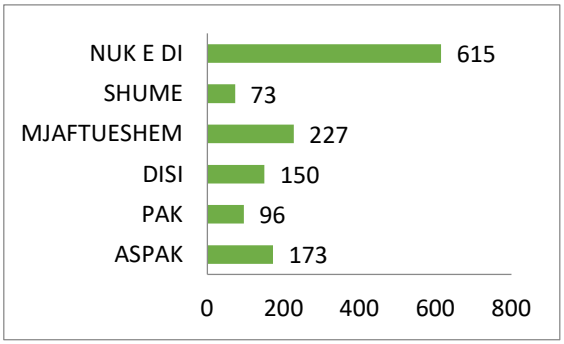


Nga këto të dhëna rezulton se 83% e të anketuarve përgjigjen se nuk janë trajnuar për sigurinë kibernetike në vendin e tyre të punës.

Ky tregues, relativisht i lartë tregon se vetë organizatat punuese nuk e vlerësojnë sigurinë kibernetike. Duke marrë parasysh se shumica e të anketuarve i përkasin sektorit publik konkludojmë për mangësi në angazhimin e strukturave shtetërore për trajnimin e punonjësve të tyre për sigurinë kibernetike në vendin e punës. Kjo shpjegon dhe përgjigjen e të anketuarve në pyetjen e mësipërme ku 47% e të anketuarve nuk ndjejnë "aspak" përgjegjësi apo që ndjejnë "pak" dhe "disi" përgjegjësi për sigurinë kibernetike në vendin e tyre të punës.

- **Gjetjet lidhur me përgjigjet e të anketuarve për pyetjen se "Nëse jeni trajnuar për sigurinë kibernetike, sa e ndjeni veten më të sigurt pas trajnimit", në paraqitje tabelore e grafike janë si më poshtë:**

Nëse po, sa e ndjeni veten më të sigurt pas trajnimit?			
		Frekuenca	%
Të Vlefshme	ASPAK	173	13.0
	PAK	96	7.2
	DISI	150	11.2
	MJAFTUESHEM	227	17.0
	SHUME	73	5.5
	NUK E DI	615	46.1
	Total	1334	100.0

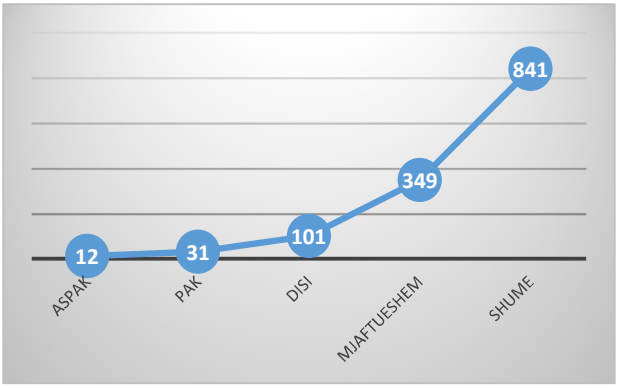


Nga analizat e gjetjeve të mësipërme statistikore mund të konkludojmë se vetëm 22.5% e të anketuarve që janë trajnuar, kanë përfituar nga ky trajnim për sigurinë kibernetike dhe e ndjejnë veten (mjaftueshëm dhe shumë) të sigurt pas trajnimit, ndërkohë që 46.1% nuk e dinë nëse kanë përfituar apo jo. Këto të dhëna tregojnë se, edhe kur janë bërë trajnime në vendin e punë lidhur me sigurinë kibernetik, ato nuk kanë qenë rezultative.

- **Gjetjet lidhur me përgjigjet e të anketuarve për fushat ku duhet investuar më shumë për të përmirësuar sigurinë kibernetike, në paraqitje tabelore dhe grafike janë si më poshtë:**

☞ **Për edukimin që në shkollë për parandalimin e krimit në internet**, si fushë ku duhet investuar për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 26.2% dhe 63%.

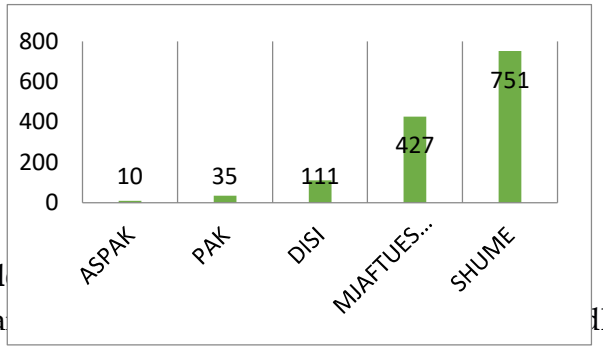
Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në edukimin që në shkollë për parandalimin e krimit në internet.			
		Frekuenca	%
Të Vlefshme	ASPAK	12	0.9
	PAK	31	2.3
	DISI	101	7.6
	MJAFTUESHEM	349	26.2
	SHUME	841	63.0
	Total	1334	100.0



☞ **Për investimin në menaxhimin e sigurisë kibernetike për të përmirësuar sigurinë kibernetike,** të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 32% dhe 56.3%.

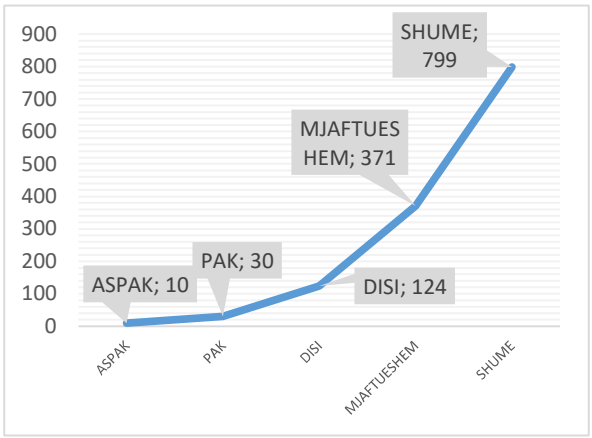
Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në menaxhimin e sigurisë kibernetike.			
		Frekuenca	%
Të	ASPAK	10	0.7

Vlefshme	PAK	35	2.6
	DISI	111	8.3
	MJAFTUESHEM	427	32.0
	SHUME	751	56.3
	Total	1334	100.0



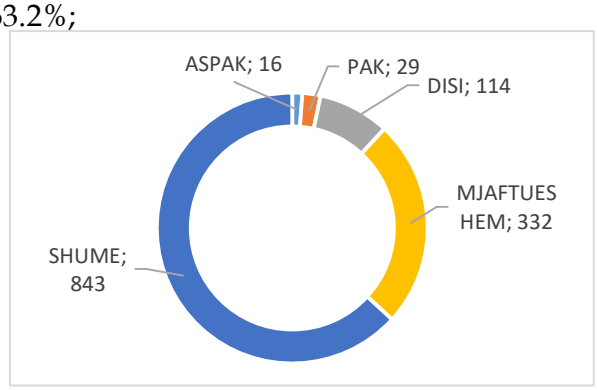
☞ **Për investimin në rritjen e nd** të përmirësuar sigurinë kibernetike, të a dhe "shumë"përkatësisht në masën 27.8% dhe 59.9%;

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në rritjen e ndërgjegjësimit të publikut të gjerë.			
		Frekuenca	%
Të Vlefshme	ASPAK	10	0.7
	PAK	30	2.2
	DISI	124	9.3
	MJAFTUES HEM	371	27.8
	SHUME	799	59.9
	Total	1334	100.0



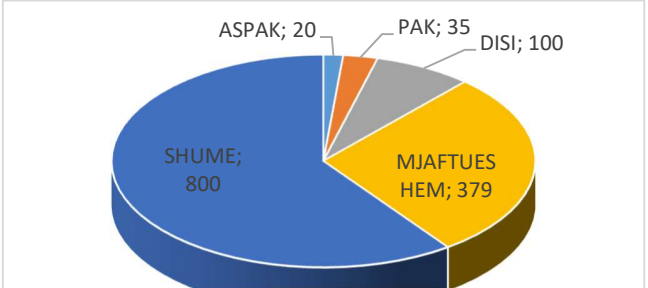
☞ **Për investimin në ligjet dhe politikat mbi krimin kibernetik** si fushë për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 24.9% dhe 63.2%;

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në ligjet dhe politikat mbi krimin kibernetik.			
		Frekuenca	%
Të Vlefshme	ASPAK	16	1.2
	PAK	29	2.2
	DISI	114	8.5
	MJAFTUES HEM	332	24.9
	SHUME	843	63.2
	Total	1334	100.0



☞ **Për investimin në rreziqet dhe efektet e krimit kibernetik** si fushë për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 28.4% dhe 60%;

☞

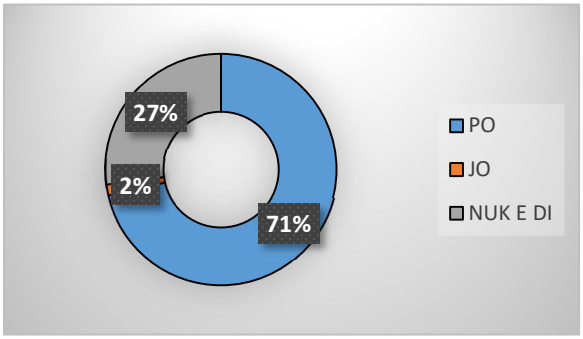


Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në rreziqet dhe efektet e krimit kibernetik.			
		Frekuenca	%
Të Vlefshme	ASPAK	20	1.5
	PAK	35	2.6
	DISI	100	7.5
	MJAFTUESHEM	379	28.4
	SHUME	800	60.0
	Total	1334	100.0

Nga analiza e gjetjeve të mësipërme, mund të konkludojmë se të anketuarit besojnë mjaftueshëm dhe shumë, në masën 87 deri 89% se fushat ku duhet investuar për të përmirësuar sigurinë kibernetike janë edukimin që në shkollë për parandalimin e krimit në internet; në menaxhimin e sigurisë kibernetike; në rritjen e ndërgjegjësimit të publikut të gjerë; në ligjet dhe politikat mbi krimin kibernetik dhe në rreziqet dhe efektet e krimit kibernetik.

- **Gjetjet për përgjigjen të anketuarve për pyetjen se nëse do të hasnit një rast të krimit kibernetik, a do ta raportonit, në paraqitje tabelore dhe grafike janë si më poshtë:**

Nëse do të hasnit një rast të krimit kibernetik, a do ta raportonit?			
		Frekuenca	%
Të Vlefshme	PO	953	71.4
	JO	20	1.5
	NUK E DI	361	27.1
	Total	1334	100.0

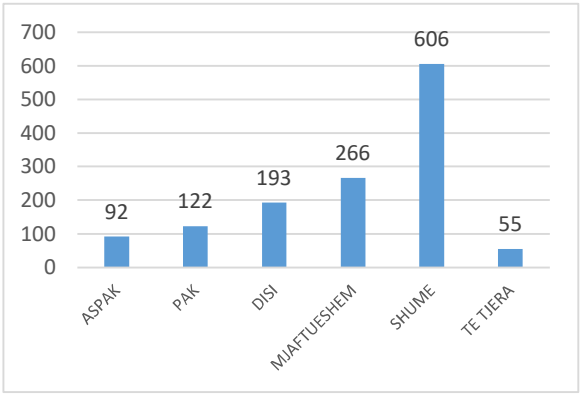


Nga analiza e gjetjeve të përgjigjeve të anketuarve për pyetjen se nëse do të hasnit një rast të krimit kibernetik, a do ta raportonit, mund të konkludojmë se shumica e të anketuarve(71.4) do ta raportonin nëse do të hasnin një rast të krimit kibernetik, përkundrejt 1.5% që nuk do ta raportonin një rast të tillë. Ndërkohë, mund të konsiderohet përsëri e lartë (27.1) shifra e atyre që janë të pavendosur për ta raportuar një rast të tillë. Për këtë rekomandohet që të gjenden mënyrat për ndërgjegjësimin edhe të kësaj kategorie për të raportuar raste e hasura të krimit kibernetik.

- **Gjetjet lidhur me përgjigjet e të anketuarve për pyetjen sa do ta raportonit një rast të krimit kibernetik në secilën nga agjencitë e mëposhtme në paraqitje tabelore dhe grafike janë si më poshtë:**

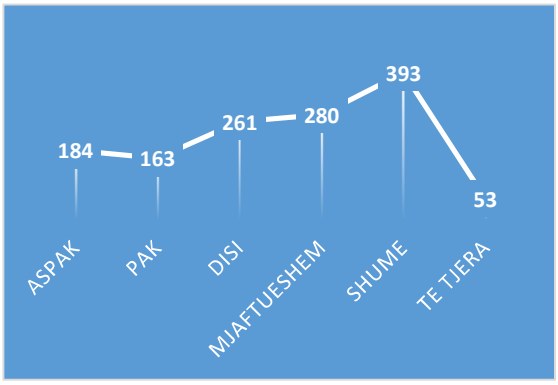
☞ **Në Policinë e Shtetit** të anketuarit do ta raportonin "disi", "mjaftueshëm" dhe "shumë " një rast të krimit kibernetik përkatësisht me 14.5%, 19.9% dhe 45.4%.

Sa do ta raportonit një rast të krimit kibernetik në Policinë e Shtetit			
		Frekuenca	%
Të Vlefshme	ASPAK	92	6.9
	PAK	122	9.1
	DISI	193	14.5
	MJAFTUESHEM	266	19.9
	SHUME	606	45.4
	TE TJERA	55	4.1
	Total	1334	100.0



▪ Në Prokurori të anketuarit do ta raportonin "disi", "mjaftueshëm" dhe "shumë" një rast të krimit kibernetik përkatësisht me 19.6%,21% dhe 29.5%.

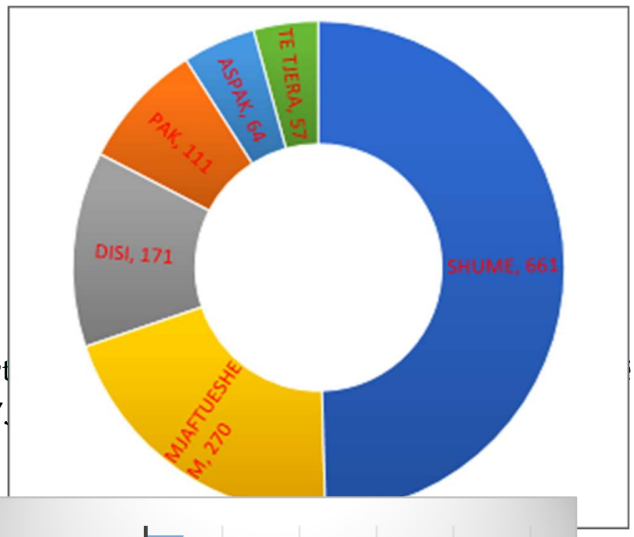
Sa do ta raportonit një rast të krimit kibernetik në Prokurori			
		Frekuenca	%
Të Vlefshme	ASPAK	184	13.8
	PAK	163	12.2
	DISI	261	19.6
	MJAFTUESHEM	280	21.0
	SHUME	393	29.5
	TE TJERA	53	4.0
	Total	1334	100.0



▪ Në Autoritetin per Sigurinë Kibernetike të anketuarit do ta raportonin "disi", "mjaftueshëm" dhe "shumë " një rast të krimit kibernetik përkatësisht me 12.8%, 20.2% dhe 49.6%.

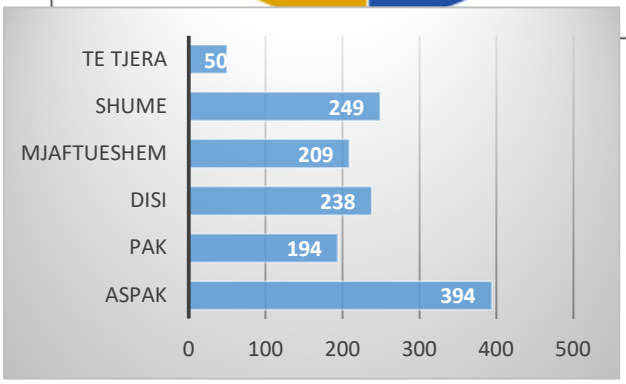
Sa do ta raportonit një rast të krimit kibernetik në Autoritetin per Sigurine Kibernetike			
		Frekuenca	%
Të Vlefshme	ASPAK	64	4.8
	PAK	111	8.3
	DISI	171	12.8
	MJAFTUE	270	20.2

	SHEM		
	SHUME	661	49.6
	TE TJERA	57	4.3
	Total	1334	100.0



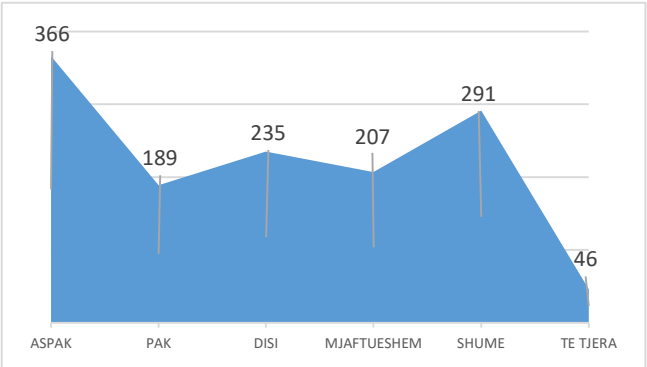
- Në SHISH të anketuarit do ta raport
rast të krimit kibernetik përkatësisht me 17.

Sa do ta raportonit një rast të krimit kibernetik në SHISH			
		Frekuenca	%
Të Vlefshme	ASPAK	394	29.5
	PAK	194	14.5
	DISI	238	17.8
	MJAFTUESHEM	209	15.7
	SHUME	249	18.7
	TE TJERA	50	3.7
	Total	1334	100.0



- Në institucionin e Avokatit të Popullit të anketuarit do ta raportonin "disi", "mjaftueshëm" dhe "shumë" një rast të krimit kibernetik përkatësisht me 17.6%, 15.5% dhe 21.8%.

Sa do ta raportonit një rast të krimit kibernetik në Avokatin e Popullit			
		Frekuenca	%
Të Vlefshme	ASPAK	366	27.4
	PAK	189	14.2
	DISI	235	17.6
	MJAFTUESHEM	207	15.5
	SHUME	291	21.8
	TE TJERA	46	3.4
	Total	1334	100.0



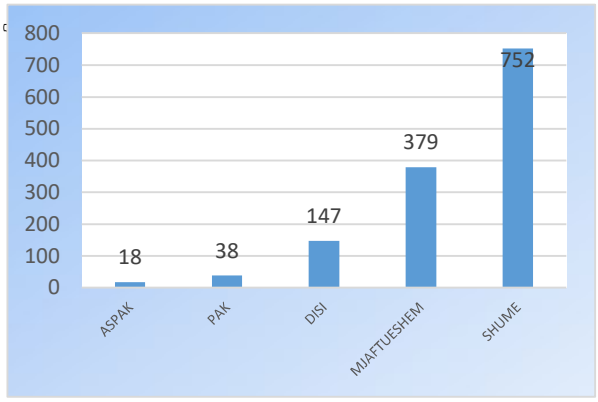
Nga gjetjet e mësipërme rezulton që nivelin më të lartë të besimit për të raportuar një rast të krimit kibernetik të anketuarit e kane tek Policia e Shtetit me 79.8%(14.5%(disi) + 19.9%(mjaftueshëm) + 45.4% (shumë)); Autoriteti Për Sigurinë Kibernetike me 82.6% (12.8%+20.2%+49.6%) dhe, më pas renditen, Prokuroria me 70.1%; Avokati i Popullit me 54.9% dhe SHISH me 52.2%.

Vlen të theksohet se ka rritje të besimit tek Autoritetit Për Sigurinë Kibernetike pas marrjes së informacionit të duhur gjatë procesit të anketimit. Kjo pasi në fillim të pyetësorit pyetjes nëse kanë raportuar apo kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK) i janë përgjigjur pozitivisht vetëm 2.1%, ndërkohë që 55% nuk kanë raportuar e kërkuar asistencë, 21.1% nuk e njohin fare atë institucion.

- **Gjetjet lidhur me përgjigjet e të anketuarve për pyetjen lidhur me alternativat që ata i vlerësojnë si hapa të domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik (pra, në rritjen e sigurisë kibernetike) në paraqitje tabelore dhe grafike janë si më poshtë:**

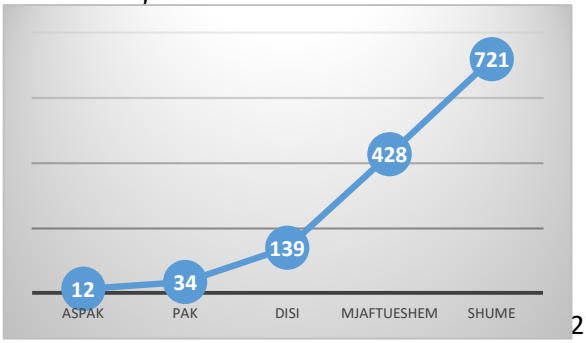
☞ **Trajnimi i duhur i oficerëve të zbatimit të ligjit** vlerësohet disi, mjaftueshëm dhe shumë si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 11%,28.4% dhe 56.4%.

Sa e vlerësoni ofrimin e trajnimit të duhur të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik si hap i domosdoshme për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	18	1.3
	PAK	38	2.8
	DISI	147	11.0
	MJAFTUESHEM	379	28.4
	SHUME	752	56.4
	Total	1334	100.0



☞ **Ritja e ndërgjegjësimit të publikut të gjerë** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 10.4%, 42% dhe 54%.

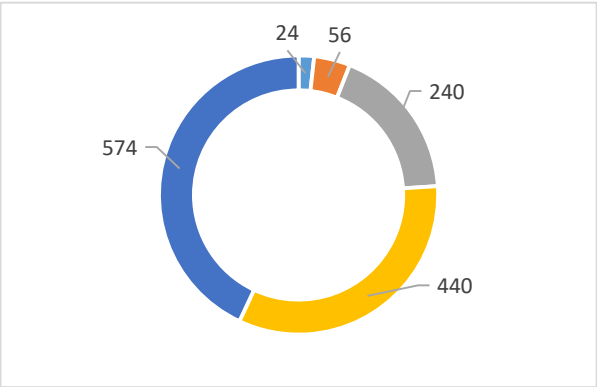
Sa i vlerësoni alternativën e rritjes së ndërgjegjësimit të publikut të gjërë si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të	ASPAK	12	.9



Vlefshme	PAK	34	2.5
	DISI	139	10.4
	MJAFTUESHEM	428	32.1
	SHUME	721	54.0
	Total	1334	100.0

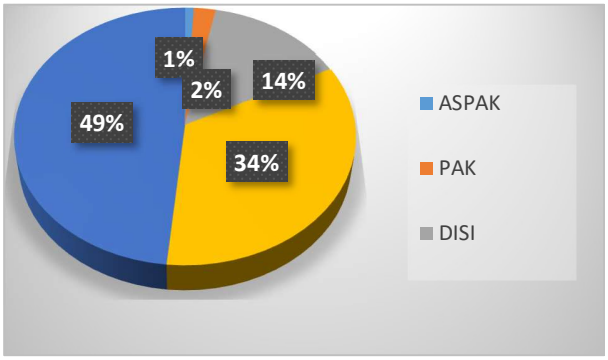
☞ **Shtimi i numrit të oficerëve të zbatimit të ligjit** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 18%, 33% dhe 43%.

Sa e vlerësoni alternativën e shtimimit të numrit të oficerëve të zbatimit të ligjit si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	24	1.8
	PAK	56	4.2
	DISI	240	18.0
	MJAFTUESHEM	440	33.0
	SHUME	574	43.0
	Total	1334	100.0



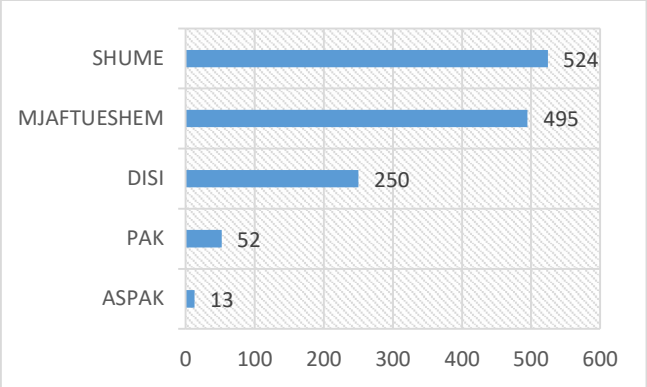
☞ **Ndryshimet e duhura ligjore** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 14%, 34.1% dhe 48.4%.

Sa e vlerësoni alternativën e ndryshimeve të duhura ligjore si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	12	.9
	PAK	30	2.2
	DISI	191	14.3
	MJAFTUESHEM	455	34.1
	SHUME	646	48.4
	Total	1334	100.0



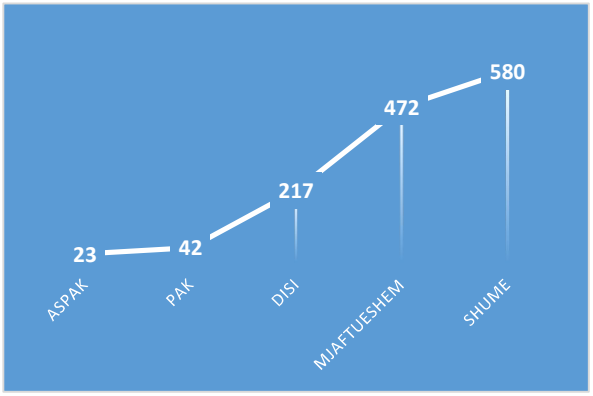
☞ **Ndryshimet e duhura strukturore** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 18.7%, 37.1% dhe 39.3%.

Sa e vlerësoni alternativën e ndryshimeve të duhura strukturore si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	13	1.0
	PAK	52	3.9
	DISI	250	18.7
	MJAFTUESHEM	495	37.1
	SHUME	524	39.3
	Total	1334	100.0



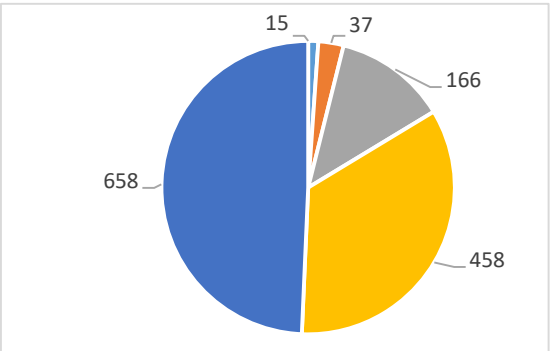
☞ **Bashkëpunimi publik-privat në fushën e luftës kundër krimit kibernetik** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 16.3%, 35.4% dhe 43.5%.

Sa e vlerësoni alternativën e rritjes së bashkëpunimit public-privat në këtë fushë si hap të domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	23	1.7
	PAK	42	3.1
	DISI	217	16.3
	MJAFTUESHEM	472	35.4
	SHUME	580	43.5
	Total	1334	100.0



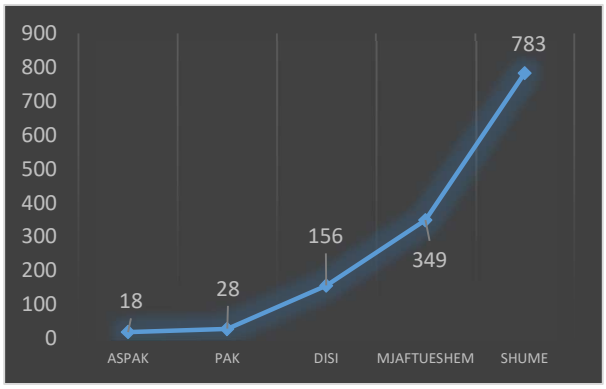
☞ **Përfshirjes së njohurive mbi veprat penale kompjuterike në programet shkollore** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 12.4%, 34.3% dhe 49.3%.

Sa e vlerësoni alternativën e përfshirjes së njohurive mbi veprat penale kompjuterike në programet shkollore si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	15	1.1
	PAK	37	2.8
	DISI	166	12.4
	MJAFTUESHEM	458	34.3
	SHUME	658	49.3
	Total	1334	100.0



☞ **Ashpërsimi i dënimeve ndaj autorëve te veprave penale kompjuterike** vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 11.7%, 26.2% dhe 58.7%,

Sa e vlerësoni alternativën e ashpërsimit të dënimeve ndaj autorëve te veprave penale kompjuterke si hap ië domosdoshme për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	18	1.3
	PAK	28	2.1
	DISI	156	11.7
	MJAFTUESHEM	349	26.2
	SHUME	783	58.7
	Total	1334	100.0



Nga analiza e gjetjeve të mësipërme mund të konkludojmë se të anketuarit i vlerësojnë si hapa të domosdoshëm për të parandaluar rritjen e rasteve të krimeve kibernetike alternativat e mësipërme në masën mbi 94% dhe konkretisht ofrimin e trajnimit të duhur të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit në masën 96.6% (11% (disi) + 28.4% (mjaftueshëm) + 56.4% (shumë); rritjen e ndërgjegjësimit të publikut të gjerë në masën 96.5%; shtimin e numrit të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik në masën 94%; ndryshimet e duhura ligjore në masën 96.8%; ndryshimet e duhura strukturore ne masën 95.1%; rritjen e bashkëpunimit publik-privat në këtë fushë në masën 95.%; përfshirjen e njohurive mbi veprat penale kompjuterike në programet shkollore në masën 96% dhe ashpërsimin e dënimeve ndaj autorëve të këtyre veprave penale në masën 96.6%. Nga alternativat e cituara më sipër rritjen e ndërgjegjësimit të publikut të gjerë në masën 96.5%;

Përfundimet dhe rekomandimet kryesore:

Në përfundim të këtij punimi është e rëndësishme të theksohet se zhvillimi i teknologjisë së sotme të informacionit dhe komunikimit po luan një luan rol gjithnjë e më të rëndësishëm në të gjithë aspektet e jetës, por tendenca për të orientuar zhvillimin ekonomik drejt teknologjive të avancuara, rrit në mënyrë të pakthyeshme varësinë nga teknologjia e cila, tashmë në terrenin e fituar, kërkon një qasje bashkëpunuese për të arritur shmangien e përdorimit të teknologjisë në kundërshtim me qëllimin kryesor . Punimi evidenton qartë pasigurinë e qytetarëve për veprimet në hapësirën kibernetike,

referuar kjo rrezikut që është prezent nga veprimet e jashtëligjshme që synojnë individin, biznesin, industrinë dhe institucionet publike. Ndërkohë niveli i vlerësimit të riskut nga individi, shoqëria dhe institucionet nuk është në shkallën me të cilin zhvillohet teknologjia dhe qasja e individit/shoqërisë ndaj saj. Kjo vjen edhe si pasojë e mungesës së duhur të informacionit, sensibilizimit, ndërgjegjësimit dhe trajnimeve në këtë fushë. Për këtë rekomandohet që fushatat sensibilizuese dhe trajnimet për kërcënimin dhe sigurinë kibernetike duhet të jenë periodike, intensive si edhe të përgatitura për të qenë të asimilueshme nga audienca të ndryshme dhe nëpër mjete te ndryshme të komunikimit, nisur kjo nga shkalla e përdorimit të teknologjisë nga këto kategori.

Më poshtë paraqiten përfundimet dhe rekomandimet kryesore nga ky punim.

- Në anketim kanë marrë pjesë nga të gjithë grupmoshat të cilave iu është adresuar pyetësori. Grupmosha 27-45 vjeç dhe 46-60 vjeç kanë qenë më të përfaqësuara në këtë anketim dhe kanë pasur më shumë interes për fushën e krimeve dhe sigurisë kibernetike. Kështu, 97.7% e kampionimit ka një nivel të lartë arsimor (bachelor, master dhe doktoraturë).
- Të anketuarit femra kanë qenë më të interesuara dhe më të ndjeshme për tematikën e anketimit, me një përgjegjshmëri më të madhe sociale se meshkujt si dhe më të sakta në plotësimin e pyetësorit nga fillimi në fund.
- Kampionimi ka një përfaqësim e larmishmëri profesionale ku numrin më të madh e përbëjnë arsimtarët (70.8%) dhe punonjësit e policisë (10%) ndërsa më pak nga bota e biznesit dhe punëtorët. Arsimtarët, si profesion, në raport me gjyqtarët, prokurorët dhe punonjësit e policisë, tregojnë një nivel përgjegjshmërie më të madhe sociale, duke u angazhuar në anketime në probleme kaq të rëndësishme për shoqërinë shqiptare, siç është krimi kompjuterik dhe siguria kibernetike.
- Shumica e të anketuarve mendojnë se zhvillimi i teknologjisë së sotme të informacionit dhe komunikimit luan rol të rëndësishëm në të gjithë aspektet e jetës duke përfshirë biznesin, komunikimin dhe edukimin, aksesin në informacion e shërbime publike dhe në fushën e privatësisë. Për shumicën e të anketuarve ky zhvillim teknologjik, cenon privatësinë ndërkohë që për një pjesë të konsiderueshme të anketuarve(31.7%) komunikimi nëpërmjet kësaj teknologjie nuk është aspak i sigurt ose është pak i sigurt.
- Sulmet me viruse, vjedhjet e identitetit dhe mashtrimet kompjuterike janë kërcënimet më të përhapura ndaj të anketuarve.
- Një numër i konsiderueshëm i të anketuarve (22.6%) kanë përjetuar pasoja të krimeve kibernetike më shumë në formën e humbjes së të dhënave kompjuterike (23.6%), vjedhje të identitetit (18%) si dhe forma të tjera të pasojave (59.9%).

- Të anketuarit nuk kanë kërkuar asistencë pranë autoritetit kryesor kombëtar të sigurisë kibernetike në rastet e përjetimit të pasojave nga krimet kibernetike. Gjithashtu, konsiderohet jo i vogël edhe numri i të anketuarve që nuk e njohin fare atë institucion.
- Të anketuarit nuk ndjehen të sigurt në aktivitetet e tyre të ndryshme në hapësirën kibernetike në masën nga 21.2% deri në 47.1%.
- Ndarja e fjalëkalimit me të tjerët si dhe përdorimi i vetëm një fjalëkalimi në të gjitha shërbimet online vlerësohet nga të anketuarit si kërcënim për sigurinë e aktiviteteve të tyre në hapësirën kibernetike.
- Në një numër të konsiderueshëm (47%) të anketuarit nuk ndjejnë "aspak" përgjegjësi apo ndjejnë "pak" dhe "disi" përgjegjësi për sigurinë kibernetike në vendin e tyre të punës.
- 83% e të anketuarve nuk janë trajnuar për sigurinë kibernetike në vendin e tyre të punës dhe vetëm 22.5% e të anketuarve që janë trajnuar, kanë përfituar nga ky trajnim për sigurinë kibernetike. Ky tregues, relativisht i lartë tregon se vetë organizatat punuese nuk e vlerësojnë sigurinë kibernetike..
- Duke marrë parasysh se shumica e të anketuarve i përkasin sektorit publik konkludojmë për mangësi në angazhimin e strukturave shtetërore për trajnimin e punonjësve të tyre për sigurinë kibernetike në vendin e punës si dhe për cilësinë e këtyre trajnimeve. Për këtë rekomandohet fillimi i trajnimit të punonjësve për sigurinë kibernetike në vendin e tyre të punës.
- Sipas të anketuarve fushat ku duhet investuar për të përmirësuar sigurinë kibernetike janë edukimin që në shkollë për parandalimin e krimit në internet; në menaxhimin e sigurisë kibernetike; në rritjen e ndërgjegjësimit të publikut të gjerë; në ligjet dhe politikat mbi krimin kibernetik dhe në rreziqet dhe efektet e krimit kibernetik.
- Shumica e të anketuarve (71.4) do ta raportonin nëse do të hasnin një rast të krimit kibernetik. Ndërkohë mund të konsiderohet përsëri e lartë (27.1) shifra e atyre që janë të pavendosur për ta raportuar një rast të tillë. Për këtë rekomandohet që të gjenden mënyrat për ndërgjegjësimin edhe të kësaj kategorie për të raportuar raste e hasura të krimit kibernetik.
- Të anketuarit do ta raportonin një rast të krimit kibernetik më shumë në Policinë e Shtetit me 79.8%(14.5%(disi) + 19.9%(mjaftueshëm) + 45.4% (shumë)); Autoriteti Për Sigurinë Kibernetike me 82.6% (12.8%+20.2%+49.6%) dhe më pas në Prokurori me 70.1%; Avokati i Popullit me 54.9% dhe SHISH me 52.2%.
- Vlen të theksohet se, pas marrjes së informacionit të duhur gjatë procesit të anketimit, ka rritje të besimit tek Autoritetit Për Sigurinë Kibernetike. Kjo pasi në

fillim të pyetësorit pyetjes nëse kanë raportuar apo kërkuar asistencë në këtë institucion i janë përgjigjur pozitivisht vetëm 2.1%, ndërkohë që 55% nuk kanë raportuar e kërkuar asistencë, 21.1% nuk e njohin fare atë institucion.

- Të anketuarit i vlerësojnë si hapa të domosdoshëm për të parandaluar rritjen e rasteve të krimeve kibernetike në masën mbi 94% ofrimin e trajnimit të duhur të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik; rritjen e ndërgjegjësimit të publikut të gjerë; shtimin e numrit të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik; ndryshimet e duhura ligjore; ndryshimet e duhura strukturore; rritjen e bashkëpunimit publik-privat në këtë fushë; përfshirjen e njohurive mbi veprat penale kompjuterike në programet shkollore si dhe ashpërsimin e dënimeve ndaj autorëve të këtyre veprave penale.
- Është e nevojshme që të studiohen dhe gjenden format e metodat e duhura për të nxitur pjesëmarrjen e punonjësve të policisë dhe me gjere në anketime të ndryshme për probleme të luftës kundër krimit, çështjeve të sigurisë dhe jo vetëm, si një shprehje e rritjes së përgjegjësisë së tyre sociale për pjesëmarrje në procesin e hartimit të politikave për këto probleme.

Literatura:

- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013.
- Informacion përmbledhës i analizave të Sektorit për Hetimin e Krimeve Kompjuterike, për vitet 2016 2018, dinamika e punës, prioritetet, kërkesat".
- Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, miratuar me VKM Nr. Nr. 973, datë 02.12.2015.
- Dokumenti për Rishikimin e Strategjisë së Mbrojtjes së Republikës së Shqipërisë. Miratuar me VKM Nr. 269, datë 03.04. 2013. Fletore Zyrtare Nr. 58, 19 Prill 2013.
- Strategjia e Sigurisë Kombëtare të Republikës së Shqipërisë, miratuar me Ligjin Nr. 103/2014.
- Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019. Republika e Kosovës, Qeveria e Kosovës, Ministria e Punëve të Brendshme. Dhjetor 2015.
- Gjetjet e anketimit të realizuar online per periudhën 7- 14 Shtator 018, me programin "Enalyzer", në adresën: https://surveys.enalyzer.com/?pid=f2q2s5r7.