kaspersky

Kaspersky Automated Security Awareness Platform (ASAP). կիբեռանվտանգության մասին իրազեկվածության բարձրացման ավտոմատացված հարթակ

www.kaspersky.ru
#իսկականանվտանգություն

Kaspersky ASAP. կիբեռանվտանգության մասին իրազեկվածության բարձրացման ավտոմատացված հարթակ

Կիբեռանվտանգության բոլոր միջադեպերի ավելի քան 80%-ը ծագում է մարդկային գործոնի պատճառով: Ձեռնարկությունները կորցնում են հսկայական միջոցներ՝ վերականգնելով ռեսուրսներն աշխատակիցների գործողությունների հետևանքով առաջացած անվտանգության խախտումներից հետո: Սակայն ուսուցման ավանդական ծրագրերը, որոնք կոչված են կանխելու նման միջադեպերը, բավականաչափ արդյունավետ չեն: Սովորաբար նրանք չեն ներշնչում մասնակիցներին և թույլ չեն տալիս նրանց մոտ ձևավորել պահանջվող վարքագիծ:

Մարդկային գործոնը՝ որպես հիմնական կիբեռռիսկ

ԱՄՆ 83 000 դոլար փոքր և միջին բիզնեսի ընկերությունների համար

Աշխատակիցների անզգուշության կամ անտեղյակության հետ կապված գրոհներից միջին վնասը[1]

ԱՄՆ 101 000 դոլար փոքր և միջին բիզնեսի ընկերությունների համար՝ ձեռնարկության հաշվով

Ֆիշինգի և սոցիալական ինժեներիայի կիրառման հետ կապված գրոհներից վնասը[1]

ԱՄՆ 400 դոլար տարեկան մեկ աշխատակցի հաշվով

Ֆիշինգային գրոհներից միջին վնասը (առանց կիբեռնսպառնալիքների այլ տեսակները հաշվի առնելու)[2]

Բոլոր կազմակերպությունների 52%-ը

Աշխատակիցների (օգտատերերի) անզգուշությունը համարում են IT-անվտանգության ապահովման ռազմավարության գլխավոր պրոբլեմ[1]

1 «Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within» (Մարդկային գործոնը IT-անվտանգությունում. ինչպես են աշխատակիցները բիզնեսը խոցելի դարձնում ներսից), «Կասպերսկի» ընկերություն և B2B International, 2017թ.

2 Տվյալները վերցված են Cost of Phishing and Value of Employee Training հետազոտությունից (Ֆիշինգի պատճառած վնասը և աշխատակիցների ուսուցման նշանակությունը), Ponemon ինստիտուտ, օգոստոս 2015թ.

Կիբեռանվտանգության մասին իրազեկության արդյունավետ բարձրացման խոչընդոտները

Ամբողջ աշխարհում ընկերությունները կիբեռսպառնալիքների մասին իրազեկվածության բարձրացման ծրագրեր են իրականացնում, բայց հաճախ աշխատակիցների ուսուցումն ու դրա արդյունքները ցանկալի արդյունք են տալիս: Առավել հաճախ դժվարությունների են բախվում փոքր և միջին բիզնեսի ձեռնարկությունները. որպես կանոն, դրանց չեն բավականացնում փորձը և հատկացված ռեսուրսները:

Անհասկանալի է, թե ինչպես պետք է սահմանել նպատակներ և պլանավորել ուսուցում

Ուսուցման կազմակերպումը շատ ժամանակ է խլում

Հաշվետվությունները չեն օգնում հետևել նպատակներին հասնելուն

Աշխատակիցները դժգոհ են ծրագրից → չեն ստանում հմտություններ

Նույնիսկ այն կազմակերպությունները, որտեղ աշխատակիցների իրազեկվածության բարձրացմամբ զբաղվում են առանձնացված աշխատանքային խմբերը, դժվարություններ են ունենում:

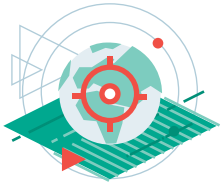
Որպես կանոն, ընկերությունները ընտրում են երկու տարբերակներից մեկը. անցկացնում են մեկանգամյա պարապմունքներ (օրինակ՝ «Կիբեռանվտանգությունը 1 ժամում») կամ լավ կառուցվածքավորված մասնագիտական ուսումնական ծրագրեր, որոնցից, սակայն, օգտագործում են միայն որոշ հիմնական գործառույթներ և գործիքներ. ֆիշինգային գրոհների նմանակման մի քանի ալիքներ մեկ տարվա ընթացքում և մի քանի ընդհանրացնող դասեր: Ուսուցման լրիվ դասընթացը շատ դժվար է լինում կազմակերպել: Որպես արդյունք՝ երկու դեպքում էլ աշխատակիցները չեն ստանում հմտություններ, որոնք անհրաժեշտ են կազմակերպության կիբեռանվտանգության ապահովման համար:

Իրազեկվածության պարզ և արդյունավետ բարձրացում ցանկացած չափի ընկերությունների համար

«Կասպերսկի» ընկերությունը ներկայացնում է կիբեռանվտանգության մասին իրազեկվածության բարձրացման սեփական ավտոմատացված հարթակը – Kaspersky Automated Security Awareness Platform (ASAP):

Պլատֆորմը առցանց գործիք է, որը ձևավորում և ամրապնդում է աշխատակիցների անվտանգ աշխատանքի հմտությունները: Դասընթացը նախատեսված է մեկ տարվա համար: Հարմար ֆունկցիոնալությունը և գործընթացի ավտոմատացումը օգնում է ընկերություններին բոլոր փուլերում՝ նպատակադրումից մինչև արդյունավետության գնահատում:

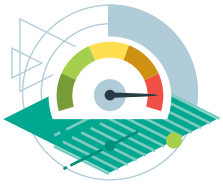
Քայլ 1.



Նպատակների սահմանում և իրազեկվածության բարձրացման անհրաժեշտության հիմնավորում

- Սահմանեք նպատակներ՝ հիմնվելով միջին գլոբալ, տարածաշրջանային կամ ոլորտային ցուցանիշների վրա:
- Ձգտեք աշխատակիցների առանձին խմբերի կիբեռհիրազեկվածության ցանկալի մակարդակի և դրան հասնելու համար անհրաժեշտ ժամանակի միջև հավասարակշռության:

Քայլ 2.



Յուրաքանչյուր աշխատակցի մոտ կարիքներին համապատասխանող հմտությունների ձևավորում

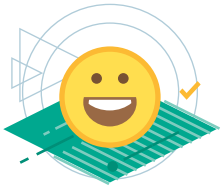
- Օգտագործեք ավտոմատացված կառավարում. հարթակը սահմանում է որոշակի աշխատակցին անհրաժեշտ հմտությունների լրակազմը, ըստ իր ռիսկի պրոֆիլի, և կառուցում ծրագիրն անցնելու ժամանակացույցը:
- Վստահ եղեք, որ ձեռք բերված հմտությունները կօգտագործվեն նյութի մանրակրկիտ ուսումնասիրման և ամրապնդման շնորհիվ:
- Աշխատակիցների իրազեկվածությունը բարձրացրեք իրենց համար հարմարավետ տեմպով՝ հաշվի առնելով նրանց ռիսկի մակարդակը և ծրագրի ինտենսիվությունը, ինչը թույլ կտա խուսափել գերհոգնածությունից և, հետևաբար, պարապմունքները շարունակելու ցանկության բացակայությունից:

Քայլ 3.

Հաշվետվությունները և վերլուծությունները՝ որպես առաջընթացին հետևելու գործիքներ

- Օպերատիվ հետևեք փոփոխություններին, միտումներին և կանխատեսումներին:
- Օգտագործեք կանխատեսումներն իրական ժամանակի ռեժիմում. դրանց օգնությամբ դուք կկարողանաք գնահատել և ժամանակին միջոցներ ձեռնարկել նպատակներին հասնելու համար:
- Գործեք առաջ լինելու ձգտումով. համակարգն ինքը կհուշի, թե որ ստորաբաժանումներին կամ առանձին աշխատակիցներին պետք է ուշադրություն դարձնել նախատեսված նպատակին հասնելու համար:
- Համեմատեք միջանկյալ արդյունքները էտալոնային ցուցանիշների հետ:

Քայլ 4.



Մոտիվացիան արդյունավետության գրավականն է

- Խաղային ձևաչափ և մրցութային մոտեցում, որոնք օգնում են հետաքրքրել աշխատակիցներին:
- Ակներև առաջադրանքներ, որոնք կիրառելի են աշխատակիցների ամենօրյա աշխատանքի համար:
- Անհատականացված մոտեցում. աշխատակիցները ստանում են միայն անհրաժեշտ գիտելիքներ իրենց հարմար տեմպով:

Պարզ կառավարում ավտոմատացման շնորհիվ

Սկսեք ընդամենը 10 րոպեում

- Անցկացրեք ընթացիկ գիտելիքների գնահատում:
- Որոշեք նպատակները՝ հաշվի առնելով միջին համաշխարհային և ոլորտային ցուցանիշները:
- Գործարկեք դասերը:
- Վճարեք միայն ակտիվ օգտատերերի համար (նրանց, ովքեր անցնում են ծրագիրը):

Պլատֆորմը գործընթացը կկառուցի աշխատակիցների տեմպին և ունակություններին համապատասխան

- Պլատֆորմը չի առաջարկի բարդ թեմաներ մինչև օգտատերը չտիրապետի հիմունքներին և հաջողությամբ չհանձնի թեստը:
- Ուսուցման համար պատասխանատու մենեջերին պետք չէ ժամանակ ծախսել յուրաքանչյուր աշխատակցի արդյունքների վերլուծության և ծրագրի լրա-կարգավորման վրա:

Ռիսկի տարբեր պրոֆիլների համար օգտագործեք տարբեր ծրագրեր

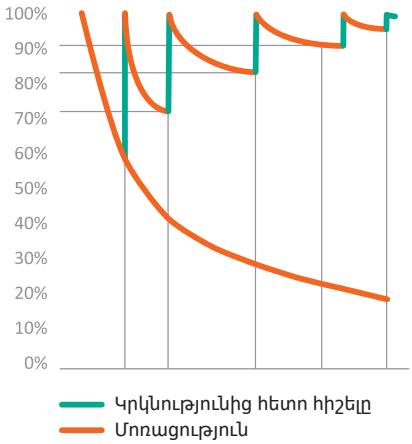
- Օգտագործեք կանոններ, որպեսզի ավտոմատ կերպով աշխատակիցներին բաշխեք տարբեր թիրախային մակարդակ և ինտենսիվություն ունեցող խմբերում, կախված գաղտնի տեղեկատվությանը հասանելիության մա-կարդակից և աշխատանքի առանձնահատկություններից:
- Դուք կարող եք օգտագործել պատրաստի խմբեր կամ ստեղծել և կարգավորել դրանք ինքներդ:

Դուք կկարողանաք ստանալ մանրամասն հաշվետվություններ ցանկացած ժամանակ

- Կառավարման վահանակում ներկայացված է առաջընթացի գնահատման հա-մար անհրաժեշտ ամբողջ տեղեկատվությունը:
- Հարթակը խորհուրդ կտա ձեզ, թե ինչ պետք է անել արդյունքը բարելավելու համար:
- Դուք կարող եք համեմատել ձեր աշխատակիցների արդյունքները հա-մաշխարհային և ճյուղային ցուցանիշների հետ:

Էբինգհաուսի կոր (մոռացության կոր)

Բազմակի կրկնությունը օգնում է ամրապնդել հմտությունները երկար ժամանակով



Պարզից բարդ

Հմտությունների մշակումը հիմնված է «պարզից բարդ» սկզբունքի վրա: Տեսական մասն անցնելուց 4 օր անց հարթակն ավտոմատ կերպով նամակներ է ուղարկում անցած նյութի հիշեցմամբ, իսկ ևս 3 օր անց առաջարկում է անցնել թեստ ստացված գիտելիքների ստուգում: Եթե թեստը հաջող է անցել, ապա որոշ ժամանակ անց օգտատերը կստանա նմանակված ֆիշինգային գրոհով նամակ: Նման մոտեցումը ապահովում է հմտությունների հուսալի ամրապնդումը և խոչընդոտում մոռանալուն:

Սովորում ենք քիչ-քիչ

- Ծրագիրը հատուկ բաժանված է կարճ պարապմունքների (2-ից 10 րոպե), քանի որ երկար և ձանձրալի դասերը կարող են հոգնեցնել ձեր աշխատակիցներին:

Գործիքների ամբողջական լրակազմ անվտանգության բոլոր բնագավառների համար

- Յուրաքանչյուր մակարդակ ներառում է. ինտերակտիվ մոդուլ և տեսանյութեր → ամրապնդման վարժություններ → ստուգում (թեստ կամ ֆիշինգային գրոհի նմանակում)

Յուրաքանչյուր թեմա բաժանվում է չորս մակարդակների, որոնք նվիրված են անվտանգության ոլորտի հմտությունների որոշակի խմբի մշակմանը: Մակարդակները համապատասխանում են տարբեր աստիճանի վտանգավորության սպառնալիքներին. առաջին մակարդակը բավական է պարզագույն և զանգվածային գրոհներից պաշտպանվելու համար, իսկ բարդ և թիրախային գրոհներից պաշտպանվելու համար անհրաժեշտ է չորրորդ մակարդակը:

Թեմաներ*

Էլեկտրոնային փոստ և ֆիշինգ

Աշխատանք ինտերնետում

Գաղտնաբառեր

Սոցիալական ցանցեր և հաղորդագրությունների փոխանակման ծառայություններ

Համակարգիչների անվտանգություն

Համակարգիչների անվտանգություն

Մոբայլ սարքեր

Գաղտնի տվյալներ

Տվյալների պաշտպանության համաեվրոպական նորմատիվներ (GDPR)

Սոցիալական ինժեներիա

Անվտանգության տանը և ճանապարհորդության ժամանակ

Օրինակ՝ հմտությունների մշակում «Ինտերնետ» թեմայի շրջանակներում

Սկզբնական մակարդակ. պաշտպանություն զանգվածային (պարզ) գրոհներից	Բազային մակարդակ. պաշտպանություն որոշակի պրոֆիլի զանգվածային գրոհներից	Միջին մակարդակ. պաշտպանություն լավ պատրաստված գրոհներից	Առաջավոր մակարդակ. պաշտպանություն թիրախային գրոհներից
13 հմտություններ, այդ թվում. – համակարգչի կարգավորում (թարմացումներ, հակավիրուս) – ակնհայտ վնասաբեր վեբ-կայքերը ճանաչելու ունակություն (այսինքն, կայքեր, որոնք առաջարկում են թարմացնել ծրագրային ապահովումը, արագացնել համակարգչի աշխատանքը, ուղարկել SMS, տեղադրել նվագարկիչներ և այլն) – վեբ-կայքերից գործարկվող ֆայլերը չբացելու սովորություն	**20 հմտություններ, այդ թվում.** – միայն վստահելի կայքերում հաշիվների գրանցում և մուտք – հրաժարում թվային հղումներով անցումից – գաղտնի տեղեկատվության մուտքագրում միայն վստահելի կայքերում – վնասակար կայքերի նշանները ճանաչելու ունակություն	**14 հմտություններ, այդ թվում.** – կեղծ հղումներ ճանաչելու ունակություն – վնասաբեր ֆայլերը և ներբեռնումները ճանաչելու ունակությունն – վնասաբեր ԾԱ-ն ճանաչելու ունակություն	**13 հմտություններ, այդ թվում.** – բարդ կեղծ հղումները ճանաչելու ունակություն (ներառյալ ձեր ընկերության կայքերի հասցեներին նման հղումները և վերաուղղորդումով հղումները) – հրաժարվում սև SEO-ով կայքեր անցումից – աշխատանքի ավարտից հետո հաշվից դուրս գալը – համակարգչի ընդլայնված կարգավորում (Java-ի անջատում, գովազդի արգելափակում, վերնակարգավորումների օգտագործում և այլն)
	+ սկզբնական մակարդակի հմտությունների ամրապնդում	+ նախկինում ձեռք բերված հմտությունների ամրապնդում	+ նախկինում ձեռք բերված հմտությունների ամրապնդում

Հիմնական հարցեր՝ հղումներ, ներբեռնումներ, ծրագրերի տեղադրում, հաշվի գրանցում և մուտք, առցանց վճարումներ, SSL

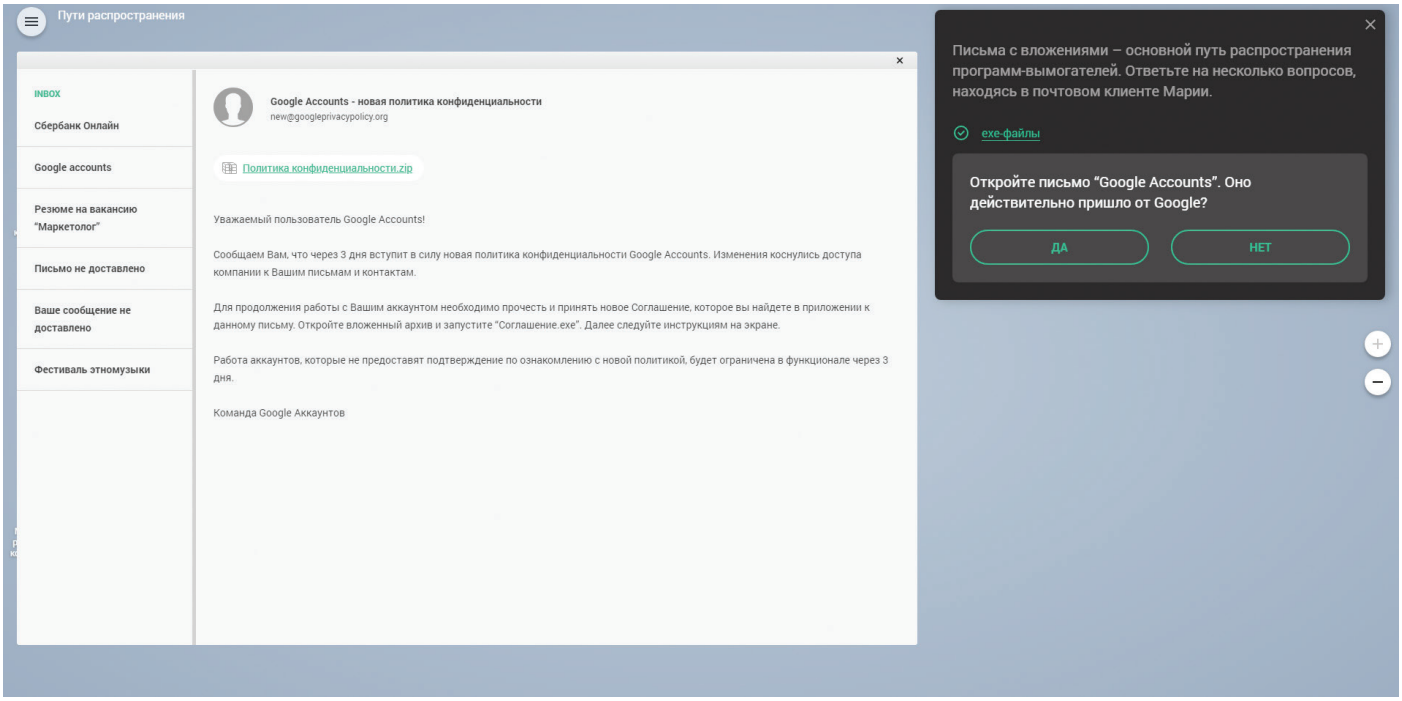
* Թեմաների վերջնական կազմը կարող է փոփոխվել առանց նախազգուշացման:

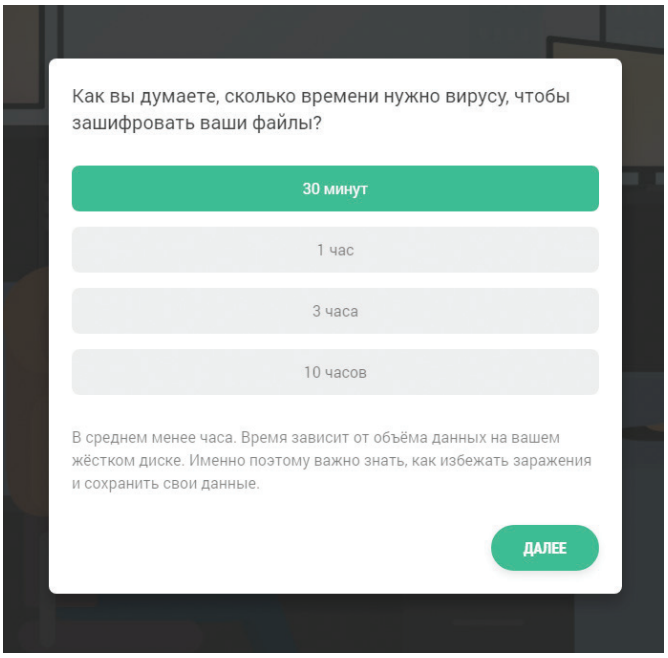
Խաղային ձևաչափ և արդիական թեմաներ

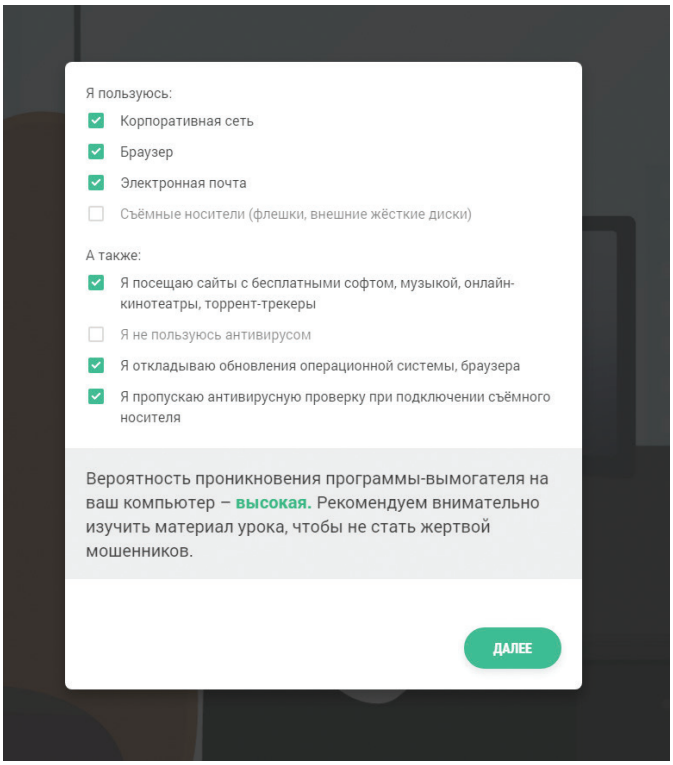
Ուսուցման հիմքում ընկած է գործնականում իրապես տեղի ունեցող իրադարձությունների նմանակումը և աշխատակիցների համար կիբեռանվտանգության անձնական նշանակալիությունը: Հարթակի նպատակն է հմտությունների ձևավորումը, այլ ոչ թե միայն գիտելիքներ փոխանցելը, ուստի գործնական առաջադրանքները յուրաքանչյուր մոդուլի անբաժանելի բաղադրիչն են:

Վարժությունների տարբեր տեսակները խթանում են օգտատերերի հետաքրքրությունը ուսուցման նկատմամբ և դրդում նրանց յուրացնել անվտանգ վարքագծի հմտությունները:

Նմանակման մեթոդը թույլ է տալիս ձևավորել գործնական հմտություններ և միաժամանակ պահպանել օգտատերերի հետաքրքրությունն ու մոտիվացիան







մինչև 90%
միջադեպերի ընդհանուր թվի կրճատում

առնվազն 50%
միջադեպերից ֆինանսական վնասի նվազեցում

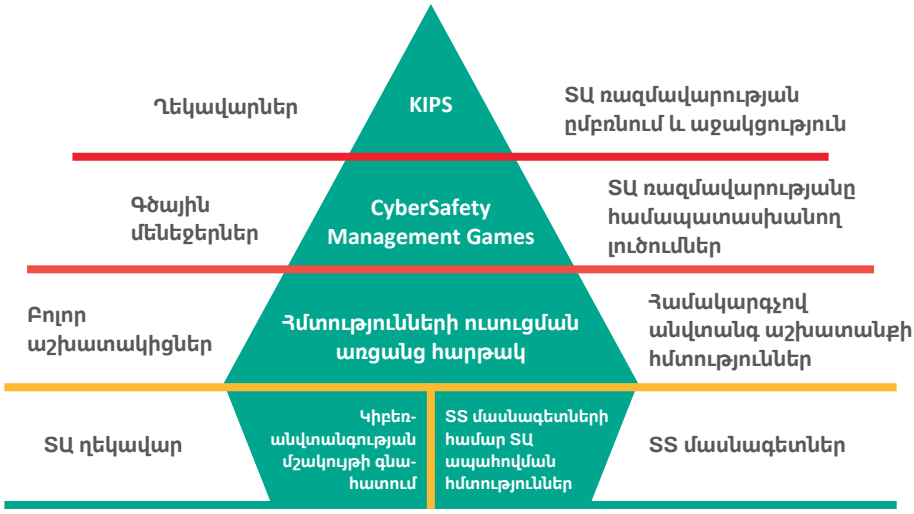
մինչև 93%
ամենօրյա աշխատանքում ստացված հմտությունների կիրառման հավանականություն

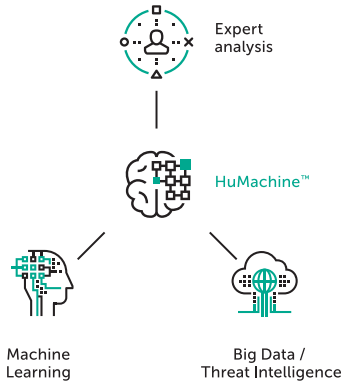
ավելի քան 30-ակի
անվտանգության մեջ ներդրումների վերադարձնելիություն

ռեկորդային 86%
մասնակիցներ պատրաստ են խորհուրդ տալ հարթակը

Kaspersky® Security Awareness

Կիբեռանվտանգության մասին իրազեկվածության բարձրացման ավտոմատացված հարթակը Kaspersky Security Awareness-ի բաղադրիչներից մեկն է: Այս պրոդուկտը ներառում է համակարգչային ուսուցման ծրագրեր տարբեր կառուցվածքային ստորաբաժանումների ներկայացուցիչների և պաշտոնների համար:





«Կասպերսկի» ընկերություն

www.kaspersky.ru

#իսկականանվտանգություն
#HuMachine