



WWW.MY.GOV.GE

ს ა ი ნ ფ ო რ მ ა ც ი ო ფ უ რ ც ე ლ ი

გამოშვება #44 ივნისი, 2015

გამოშვებაში წაიკითხავთ

- 1 რეგიონული სამუშაო შეხვედრა
- 2 „ღია მმართველობის პარტნიორობის“ რეგიონული კონფერენცია
- 3 მონაცემთა გაცვლის სააგენტოს ვორქშოპი „ღია მმართველობის პარტნიორობის“ რეგიონული კონფერენციის ფარგლებში
- 3 სომხეთ-საქართველოს სამართლებრივი თანამშრომლობის ფორუმი
- 4 მონაცემთა გაცვლის სააგენტოს წარმომადგენლების ვიზიტი გერმანიაში
- 4 **GOOGLE**-ს რუკაზე თბილისის მონაცემები სრულად განთავსდა

მონაცემთა გაცვლის სააგენტომ „NATO“-სთან თანამშრომლობით კიბერუსაფრთხოების საკითხებზე რეგიონული სამუშაო შეხვედრა გამართა



საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტომ „NATO“-ს პროგრამის - „მეცნიერება მშვიდობისა და უსაფრთხოებისთვის“ (SPS) - ფარგლებში სასტუმრო „რუმს ჰოტელ თბილისში“ პირველი რეგიონული სამუშაო შეხვედრა გამართა, რომელიც კიბერუსაფრთხოების საკითხებში თანამშრომლობის გაუმჯობესებული საშუალებების იდენტიფიცირებასა და სამხრეთ კავკასიისა და შავი ზღვის აუზის ქვეყნებში რეგიონული კიბერთავდაცვის უზრუნველყოფას მიეძღვნა.

ლონისძიება გახსნა და მონაწილეებს სიტყვით მიმართა საქართველოს იუსტიციის მინისტრმა **თეა წულუკიანმა**, რომელმაც ხაზი გაუსვა მონაცემთა გაცვლის სააგენტოს ინიციატივითა და „NATO“-ს ეგიდით გამართული სამუშაო შეხვედრის მნიშვნელობას რეგიონში კიბერუსაფრთხოების მაღალი დონის მისაღწევად.

საქართველოს მთავრობის მხრიდან ღონისძიების ინიციატორმა და ორგანიზატორმა, საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტომ, სამუშაო შეხვედრაში მონაწილეობის მისაღებად თავი მოუყარა 18 ქვეყნის 50-ზე მეტ წარმომადგენელს. ვორქშოპს ესწრებოდნენ „NATO“-ს წევრი ქვეყნების კიბერუსაფრთხოების სფეროს ექსპერტები, ასევე სხვადასხვა საერთაშორისო ორგანიზაციისა და საქართველოში კიბერ და ინფორმაციული უსაფრთხოების მიმართულებით მომუშავე ყველა უწყების წარმომადგენლები, რომლებმაც განიხილეს რეგიონში კიბერთავდაცვის სფეროში ინსტიტუციონალური შესაძლებლობების განვითარების საშუალებები, კიბერინციდენტების, მათზე პროგრამებისა და კიბერუსაფრთხოების განეიტრალების თანამედროვე მეთოდები და ამ მიმართულებით თანამშრომლობის გაღრმავების პერსპექტივები (გაგრძელება გვ. 2).

(გაგრძელება. დასაწყისი გვ. 1)

„ეს არის პირველი შემთხვევა, როდესაც საქართველოში „NATO“-ს მონაწილეობით იმართება ასეთი მაღალი დონის სამუშაო შეხვედრა, რომელიც მთლიანად კიბერუსაფრთხოების საკითხებს ეხება. ეს NATO-ს წევრ ქვეყნებთან ჩვენი წარმატებული მუშაობის შედეგია. მაგალითად, წლების განმავლობაში მონაცემთა გაცვლის სააგენტოს წარმომადგენლები „NATO“-ს პროგრამის - „მეცნიერება მშვიდობისა და უსაფრთხოებისთვის“ - ფარგლებში წარმატებით ატარებდნენ ტრენინგებს სხვადასხვა ქვეყნის კიბერ და ინფორმაციული უსაფრთხოების სპეციალისტებისთვის, გვქონდა აქტიური თანამშრომლობა კიბერინციდენტების ერთობლივად განეიტრალების მიმართულებითაც. ყოველივე ამის შედეგად, დღეს ჩვენ თანამშრომლობის თვისებრივად



ახალ ეტაპზე გადავდით, როდესაც „NATO“-ს ეგიდით თბილისში თავი მოვუყარეთ დარგის ცნობილ ექსპერტებსა და სპეციალისტებს, რაც საშუალებას გვაძლევს გამოცდილება და ცოდნა გავუზიაროთ ერთმანეთს, ხოლო საქართველო, როგორც კიბერ და ინფორმაციული უსაფრთხოების თვალსაზრისით რეგიონული ცენტრი, კიდევ უფრო დაუახლოვდეს ჩრდილოატლანტიკურ ალიანსს“, - **ირაკლი გვენეტაძე**, საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს თავმჯდომარე.

ლონისძიების ორგანიზებაში, რომელიც 30 ივნისიდან 1 ივლისამდე მიმდინარეობდა, ასევე ჩართული იყო კომპანია „ინტელიუმი“ - გლობალური საკონსულტაციო ფირმა, რომლის საქმიანობის სფეროა დაეხმაროს საჯარო და კერძო ორგანიზაციებს სწორად შეიმუშაონ და განავითარონ კიბერუსაფრთხოების სტრატეგიები.

„ღია მმართველობის პარტნიორობის“ ევროპის რეგიონული კონფერენცია თბილისში



3-4 ივნისს თბილისში „ღია მმართველობის პარტნიორობის“ (OGP) ევროპის რეგიონული კონფერენცია გაიმართა. 2 დღის განმავლობაში 40-მდე ქვეყნის წარმომადგენლები სამთავრობო უწყებებიდან და საერთაშორისო ორგანიზაციებიდან ღია და გამჭვირვალე მმართველობის საკითხებზე ერთმანეთს საკუთარ გამოცდილებას უზიარებდნენ.

კონფერენცია საქართველოს პრემიერ-მინისტრმა **ირაკლი ღარიბაშვილმა** გახსნა. ოფიციალური ცერემონიის დასრულების შემდეგ სტუმრებმა საკონფერენციო სივრცის

შოურუმები დაათვალიერეს, სადაც იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედმა ექვსმა საჯარო სამართლის იურიდიულმა პირმა, მთავრობის ადმინისტრაციამ, საჯარო სამსახურის ბიურომ და შინაგან საქმეთა სამინისტრომ ელექტრონული სერვისები წარმოადგინეს.

„ღია მმართველობის პარტნიორობის“ ევროპის რეგიონული კონფერენციის ფარგლებში საქართველომ და საფრანგეთმა თანამშრომლობის დოკუმენტები გააფორმეს. ქართული მხრიდან დოკუმენტებს ხელი მოაწერა საქართველოს იუსტიციის მინისტრმა **თეა წულუკიანმა**, ხოლო ფრანგული მხრიდან – საფრანგეთის სახელმწიფო მინისტრმა რეფორმებისა და სახელმწიფო სერვისების გამარტივების დარგში **ტიერი მანდონმა**.

„ღია მმართველობის პარტნიორობის“ ევროპის რეგიონული კონფერენციის ფარგლებში მონაცემთა გაცვლის სააგენტომ ვორქშოპი გამართა



„ღია მმართველობის პარტნიორობის“ ევროპის რეგიონული კონფერენციის მეორე დღე საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს ვორქშოპით გაიხსნა, რომელზეც სააგენტოს თავმჯდომარემ, ირაკლი გვენეტაძემ პრეზენტაცია გააკეთა მომავლის ელექტრონულ სერვისებზე და ისაუბრა მათი გამოყენების შედეგად მიღებულ შესაძლო სარგებელზე, რომელსაც მიიღებს როგორც სახელმწიფო, ისე მოქალაქე.

პრეზენტაციის შემდეგ სამუშაო ჯგუფებად დაყოფილმა აუდიტორიამ საკუთარი ხედვა წარმოადგინა თანამედროვე ინფორმაციული

ტექნოლოგიების გამოყენებით სხვადასხვა აპლიკაციისა და პლატფორმის შექმნასთან დაკავშირებით, რომლის მოხმარებაც გაზრდის მოქალაქეების ჩართულობას საჯარო მმართველობის განხორციელების პროცესში, გაადვილებს სახელმწიფო სტრუქტურებისგან ელექტრონული სერვისების მიღებას და ხელს შეუწყობს ელექტრონული მმართველობის განვითარებას.

„სამუშაო სესიაზე ჯგუფებად დაყოფილ აუდიტორიას ვთხოვეთ წარმოედგინათ საკუთარი კონცეფცია ისეთ სერვისებთან დაკავშირებით, რომლებსაც სამომავლოდ პრაქტიკული გამოყენება ექნებოდათ და სარგებელს მოუტანდნენ როგორც სახელმწიფოს, ისე მოქალაქეებს და, რაც მთავარია, ეს სერვისები დაფუძნებული იქნებოდა თანამედროვე ტექნოლოგიებზე. თითოეულმა ჯგუფმა საინტერესო იდეები ჩამოაყალიბა, რაც გვაძლევს იმის თქმის შესაძლებლობას, რომ სამუშაო სესიამ წარმატებულად ჩაიარა“, - აღნიშნა **ირაკლი გვენეტაძემ**, საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს თავმჯდომარემ.

ღია მმართველობის პარტნიორობის ევროპის რეგიონული კონფერენცია ამა წლის 3-4 ივნისს მიმდინარეობდა.

სომხეთ-საქართველოს სამართლებრივი თანამშრომლობის ფორუმი



იუსტიციის სამინისტროს დელეგაციამ იუსტიციის მინისტრის ხელმძღვანელობით სომხეთ-საქართველოს სამართლებრივი თანამშრომლობის ფორუმში მიიღო მონაწილეობა, რომელიც ერევანში 25-26 ივნისს გაიმართა.

ფორუმის ფარგლებში რამდენიმე სესია მუშაობდა. პირველ თემატურ სესიაზე სერვისების ხელმისაწვდომობის, ინფორმაციის თავისუფლებისა და ელექტრონული მმართველობის საკითხები განიხილეს. ამავე სესიაზე საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს თავმჯდომარემ, **ირაკლი გვენეტაძემ** გააკეთა პრეზენტაცია საქართველოში ელექტრონული მმართველობის განვითარების ეტაპებისა და ელექტრონული სერვისების ხელმისაწვდომობის

თემაზე. მეორე სესიის თემა საქართველოში არასრულწლოვანთა მართლმსაჯულების რეფორმა იყო. საუბარი შეეხო პენიტენციარულ სფეროს, დანაშაულის პრევენციას და პატიმართა რესოციალიზაცია-რეაბილიტაციას. კიდევ ერთი სფერო, რომელსაც სესია მიეძღვნა, „ღია მმართველობის პარტნიორობასთან“ დაკავშირებული საკითხებია. გარდა ამისა, საქართველოს იუსტიციის სამინისტროს დელეგაციის წევრებმა ფორუმის მონაწილეებს იუსტიციის სახლებისა და საზოგადოებრივი ცენტრების კონცეფციასაც გააცნეს.

მონაცემთა გაცვლის სააგენტოს წარმომადგენლების ვიზიტი გერმანიაში



2015 წლის 9-12 ივნისს, საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს წარმომადგენლები სამუშაო ვიზიტით იმყოფებოდნენ გერმანიის ფედერაციულ რესპუბლიკაში. ვიზიტის ფარგლებში გაიმართა შეხვედრები გერმანიის ელექტრონული მმართველობის კომპეტენციების ცენტრების წარმომადგენლებთან მათი გამოცდილების გაზიარების მიზნით.

კომპეტენციის ცენტრი წარმოადგენს არასამთავრობო ორგანიზაციას, რომლის დამფუძნებლებიც არიან

ელექტრონული მმართველობის სფეროში კომპეტენტური მკვლევარები და საჯარო მოხელეები. ცენტრი 2014 წელს დაარსდა და 60 პროფესიონალს აერთიანებს.

ცენტრის მუშაობა ფოკუსირებულია ელექტრონული მმართველობის სფეროში განხორციელებულ კვლევებზე, საჯარო სექტორის მხარდაჭერაზე, სატრენინგო და საკონსულტაციო სერვისების შეთავაზებაზე. ცენტრი ასევე ახორციელებს კვლევით პროექტს - „100 ყველაზე გამოყენებადი სახელმწიფო ელექტრონული სერვისი“.

ვიზიტის ფარგლებში ასევე გაიმართა შეხვედრა კომპანია „ფოკუსის“ ოფისში, რომლის წარმომადგენლებმაც გააკეთეს პრეზენტაცია კომპანიის ძირითადი მიმართულებებისა და მნიშვნელოვანი პროექტების შესახებ.

აღნიშნული კომპანია ფოკუსირებულია ელექტრონული მმართველობის სფეროში ელექტრონული სერვისების შემუშავებასა და ინფორმაციული სისტემების დანერგვაზე. მათგან აღსანიშნავია პორტალი, რომელიც სერვისების მიღებას ერთი ფანჯრის პრინციპით ხდის შესაძლებელს.

GOOGLE-ს რუკაზე თბილისის მონაცემები სრულად განთავსდა



რეესტრის ეროვნული სააგენტო Google map-ზე დაიწყო, გორი იქნება.

საჯარო რეესტრის ეროვნული სააგენტო უკვე მესამე წელია სივრცით (გეოგრაფიულ) მონაცემებს აგროვებს და მუდმივად მუშაობს, რომ მსოფლიოში ერთ-ერთ ყველაზე პოპულარულ საძიებო სისტემაში საქართველოსთან დაკავშირებული ინფორმაცია სრულყოფილად იყოს ასახული. რუკას თანდათან ემატება შენობები, გზები, მისამართები, ინფორმაცია დასახლებული პუნქტების, ქუჩების, საავტომობილო გზების, სარკინიგზო მაგისტრალების, მთების, მწვერვალების, მდინარეებისა და სხვადასხვა ღირსშესანიშნაობის შესახებ.

Google-ს პოპულარულ საძიებო სისტემაში საქართველოს შესახებ სრული ინფორმაციის განთავსება მნიშვნელოვანია, როგორც ზოგადად ქვეყნის პოპულარიზაციისთვის, ასევე ნავიგაციის სისტემის, ტურიზმისა და ქვეყნის ეკონომიკური განვითარებისთვის.

საჯარო რეესტრის ეროვნულმა სააგენტომ Google-ს რუკაზე თბილისის მონაცემების გადატანა დაასრულა. ინტერაქტიულ რუკაზე სრულად განთავსდა ინფორმაცია დედაქალაქში არსებული ყველა შენობა-ნაგებობისა და გზათა ქსელის შესახებ. აღნიშნული მონაცემები დაახლოებით 3500 კილომეტრის სიგრძის გზათა ქსელს და 160 ათას შენობა-ნაგებობას აერთიანებს, რომლებიც შესაბამისი სამისამართო ნუმერაციითაა დანომრილი.

ამერიიდან ყველა დაინტერესებულ პირს საშუალება აქვს, Google-ს რუკაზე მოიძიოს თბილისში არსებული ნებისმიერი შენობა, მათ შორის ყველა საგანმანათლებლო დაწესებულება: საჯარო და კერძო სკოლები, უმაღლესი და პროფესიული სასწავლებლები.

მომდევნო ქალაქი, რომლის მონაცემების ასახვასაც საჯარო

CERT.GOV.GE-ს რეკომენდაციები

ფიშინგი



ფიშინგი (ინგლისურად phishing: fishing - თევზაობა) — ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პირადი საიდენტიფიკაციო მონაცემები, მაგალითად, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია.

ფიშინგის მეშვეობით შენიღბული ინტერნეტ კომუნიკაციის საშუალებით ხდება მომხმარებლის შესახებ ისეთი ინფორმაციის მოპოვება, როგორცაა მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი. ეს მიიღწევა შემდეგი მეთოდებით: მასიური ელექტრონული წერილების დაგზავნით (წერილის ავტორებად იყენებენ ცნობილ ორგანიზაციებსა და ბრენდებს); პირადული შეტყობინებებით, როდესაც გამოყენებულია

ცნობილი ბანკის სახელი; სოციალური ქსელების საშუალებებით. ასეთ წერილში ხშირად არის ვებგვერდის ბმული, რომლის ვიზუალური მხარე არ განსხვავდება ნამდვილისგან. შესაბამისად, გაყალბებულ ვებგვერდზე შეტანილი ინფორმაცია - მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი - ავტომატურად ხვდება ე.წ. "ფიშერის" ხელში.

ფიშინგის ისტორია: პირველი სტატია ფიშინგზე და ფიშინგის განხორციელების მეთოდებზე 1996 წელს გამოქვეყნდა ე.წ. ჰაკერულ ჟურნალში - "2600: The Hacker Quarterly".

ახალი საფრთხეები: დღევანდელ დღეს ფიშინგი აღარ არის უბრალოდ ინტერნეტ-თაღლითობა. ყალბი ვებგვერდების არსებობა გახდა თაღლითობის მრავალი მიმართულებიდან ერთ-ერთი ყველაზე აქტუალური და საგანგაშო. წერილი, რომელიც თითქოს ბანკიდან არის გამოგზავნილი, შეიძლება მომხმარებელს მოუწოდებდეს მითითებულ ნომერზე სავალდებულო დაკავშირებისკენ, რათა მოგვარდეს მის საბანკო ანგარიშზე არსებული პრობლემა. ამ მეთოდს ეწოდება ვიშინგი "ViShing" (ხმოვანი ფიშინგი). აღნიშნულ ნომერზე დარეკვის შემდეგ, მომხმარებელი ხვდება ავტო მოპასუხესთან, რომელიც ითხოვს ინფორმაციას სხვადასხვა პირად მონაცემზე, მაგალითად, პინ-კოდზე, ანგარიშის ნომერზე, პაროლებზე და ა.შ. ასევე "ვიშერები" თავადაც რეკავენ მსხვერპლთან და არწმუნებენ მათ, რომ ისინი ოფიციალური ორგანიზაციიდან არიან, რისთვისაც იყენებენ ყალბ სატელეფონო ნომრებს. შედეგად ისინი ახერხებენ მომხმარებლის პირადი ინფორმაციის მოპოვებას.

ასევე ძალიან პოპულარული ხდება სმს ფიშინგი, რომელიც ცნობილია, როგორც სმიშინგი "SMiShing". თაღლითები თავის მსხვერპლს უგზავნიან სმს შეტყობინებას, რომელშიც მოთავსებულია ფიშინგ საიტის ბმული. ბმულზე შესვლისას მომხმარებელი ხდება ფიშერის მსხვერპლი და კარგავს პირად ინფორმაციას. სმს შეტყობინება ასევე შეიძლება მოუწოდებდეს მომხმარებელს პრობლემის მოგვარების მიზნით მითითებულ ნომერზე დაუყოვნებლივ დაკავშირებისკენ.

ფიშინგ წერილი - ფიშინგ წერილი არის ელექტრონული ფოსტის მისამართზე მოსული ყალბი წერილი, რომელიც თითქოს გამოგზავნილია ბანკის, სერვისის პროვაიდერის ან სხვა ცნობილი ორგანიზაციის მიერ, რომელთანაც მომხმარებელს აქვს შეხება. წერილის მიმღებს რაიმე მიზეზით სთხოვენ განაახლოს თავისი პირადი მონაცემები მითითებული ბმულის საშუალებით. დასახელებული მიზეზი შეიძლება იყოს სხვადასხვაგვარი. მაგალითად, ყალბი წერილი შეიძლება იტყობინებოდეს, რომ მომხმარებლის ანგარიში დაიბლოკვება, თუ არ მოხდება მისი პაროლის ან საკრედიტო ბარათის ინფორმაციის განახლება.

ფიშინგ წერილების დამახასიათებელი ნიშანია მაღალი ხარისხის გაყალბება. მაგალითად, მიმღები იღებს წერილებს ბანკის ან სერვის პროვაიდერის ლოგოთი, რომელიც არის ორიგინალის ზუსტი ასლი და მომხმარებელი გადადის არა ოფიციალურ ვებგვერდზე, არამედ ყალბზე, რომელიც ვიზუალურად ცნობილი კომპანიის ვებგვერდის იდენტურია - მხოლოდ მისამართია განსხვავებული და ინფორმაციის შეგროვების შემდეგ შეიძლება მოხდეს მომხმარებლის გადამისამართება რეალურ ვებგვერდზე.

ფიშინგ ვებგვერდის ფუნქცია - მომხმარებელი გადადის ყალბ ვებგვერდზე და მითითებულ ველებში უთითებს საკუთარ სახელს, პაროლსა და საბანკო რეკვიზიტებს, რითაც ეს მონაცემები თაღლითებისთვის ხდება ხელმისაწვდომი. აღსანიშნავია ისიც, რომ ყველა "ფიშერი" თავად არ იყენებს მოპოვებულ ინფორმაციას, არამედ ყიდიან სხვა პირებზე, რომლებსაც აქვთ კარგად შემუშავებული გეგმა თუ როგორ უნდა მოიპარონ ფული სხვისი ანგარიშებიდან (გაგრძელება გვ. 6).

(გაგრძელება. დასაწყისი გვ. 5)

როგორც წესი, ფიშინგ ვებგვერდი ფუნქციონირებს მხოლოდ რამოდენიმე დღე (საშუალოდ 5-10), რადგან ანტი-ფიშინგ ფილტრები დროულად პოულობენ ახალ საშიშროებებს და ამის გამო ფიშერებს უწევთ ახალ-ახალი ვებგვერდების რეგისტრაცია ან უკვე არსებული სხვა ვებგვერდების გატეხვა და მალულად ფიშერული საიტის განთავსება.

როგორ ხორციელდება ფიშინგი - ფიშინგის ყველაზე ხშირ სამიზნეს წარმოადგენენ ბანკები, საფინანსო ორგანიზაციები, ელექტრონული აუქციონები და ინტერნეტ მაღაზიები, რადგან თაღლითებს სურთ მოიპოვონ ისეთი ინფორმაცია, რომელიც ფულთან წვდომის საშუალებას იძლევა. ასევე პოპულარულია ელექტრონული ფოსტის მონაცემების მოპარვა, რათა შემდგომში გამოიყენონ სპამისა და ვირუსების გასავრცელებლად.

პირადი მონაცემების მოპარვა არ არის ერთადერთი საფრთხე, რომელიც მომხმარებელს შეიძლება დაემუქროს. ფიშინგური ვებგვერდი შეიძლება ასევე შეიცავდეს მავნე ან ჯამშუმურ პროგრამას. თუ თქვენ არ გაქვთ არანაირი ანგარიში, რომლითაც შეიძლება თაღლითები დააინტერესდნენ, ეს არ ნიშნავს, რომ თქვენ უსაფრთხოდ ხართ, რადგან ფიშინგური შეტევების წარმატება დაფუძნებულია მომხმარებელთა გაუთვითცნობიერებულობაზე ან უყურადღებობაზე.

ფიშერები ხშირად ტექსტის ნაცვლად გამოსახულებას იყენებენ, რის შემდეგაც ანტიფიშინგის ფილტრებს ურთულდებათ მათი აღმოჩენა, მაგრამ სპეციალისტებმა შეიმუშავეს მეთოდი, რომელიც ელექტრონულ წერილში მოსულ გამოსახულებას ადარებს ანტიფიშინგის ბაზას და მხოლოდ მას შემდეგ ბლოკავს მას, თუ აღმოაჩენს ფიშინგის ელემენტებს.

ინტერნეტ ბრაუზერები, რომლებიც იუწყებიან ფიშინგის საფრთხეს - ძალიან მნიშვნელოვანი მიმართულებაა ფიშინგ საიტების სიის შექმნა (ე.წ. „ბლეკლისტი“), რომელსაც აქტიურად იყენებენ ისეთი ინტერნეტ ბრაუზერები, როგორებიცაა Internet Explorer, Mozilla Firefox, Google Chrome, Safari და Opera. 2006 წელს შეიქმნა DNS სერვისების მეთოდი, რომელიც ფილტრავს ცნობილ ფიშინგ საიტებს. ეს მეთოდი მუშაობს ყველა ზემოჩამოთვლილ ინტერნეტ ბრაუზერში.

ფიშინგთან ბრძოლა - რამდენიმე წლის წინ ფიშინგთან საბრძოლველად შეიქმნა ანტი-ფიშინგის სამუშაო ჯგუფი (Anti-Phishing Working Group - APWG), რომელშიც გაერთიანებული არიან ფიშინგის სამიზნე კომპანიები, ასევე უსაფრთხოების პროგრამული უზრუნველყოფის მწარმოებლები და კიბერდანაშაულთან მებრძოლი კომპანიები - სულ 2500 კომპანიაზე მეტი. APWG-ს წევრები ერთმანეთს ატყობინებენ ახალი ფიშერული შეტევების შესახებ და ერთად ზრუნავენ ამ საკითხთან დაკავშირებით საზოგადოების ცნობიერების ამაღლებაზე.

ობილეთ ჩვენი საიტები

www.dea.gov.ge; www.my.gov.ge

მონაცემთა გაცვლის
სააგენტო

წმ. ნიკოლოზის/ნ. ჩხეიძის ქ. 2
თბილისი 0102, საქართველო
ტელეფონი: (+ 995 32) 291 51 40
ელ.ფოსტა: info@dea.gov.ge

საქართველოს იუსტიციის სამინისტრო

მონაცემთა გაცვლის
სააგენტო



თუ ხართ ახალი მომხმარებელი ან კვლავ გსურთ საინფორმაციო ფურცლის გამოწერა, გთხოვთ გამოაგზავნოთ ელექტრონული შეტყობინება მისამართზე: info@dea.gov.ge და სათაურში მიუთითოთ “Subscribe” ან დაარეგისტრირდით თქვენი ელექტრონული ფოსტის მისამართი ვებ გვერდზე: www.e-government.ge

თუ არ გსურთ, მონაცემთა გაცვლის სააგენტოს საინფორმაციო ბიულეტენის მიღება, გთხოვთ