# კიბერდანაშაული

## სამართლებრივი კულტურა

Government of the United States

PH international
ADVANCING SOCIETIES, CONNECTING PEOPLE

# გაკვეთილის მიზნები

**მოსწავლე შეძლებს:**

- ერთმანეთისგან განასხვაოს კიბერდანაშაული და კიბერმეთოდებით ჩადენილი დანაშაული შემთხვევების განხილვის გზით.
- ჩამოთვალოს, ერთმანეთისგან განასხვაობს და იმსჯელოს საქართველოში გავრცელებული კიბერდანაშაულისა და იმ საფრთხეების შესახებ, რომლის წინაშეც შეიძლება აღმოჩნდეს კიბერდანაშაულის მსხვერპლი;
- ჩამოთვალოს და იმსჯელეოს კიბერდანაშაულის თავიდან არიდების გზების შესახებ;
- განსახილველ შემთხვევებთან მიმართებაში გაანალიზოს საქართველოს სისხლის სამართლის კოდექსის ის მუხლები, რომლებიც არეგულირებს კიბერდანაშაულს;
- მიიღოს ინფორმაცია იმ სახელმწიფო უწყებების შესახებ, რომლებიც ჩართულნი არიან კიბერდანაშაულის გამოძიების პროცესში;
- მიიღოს ინფორმაცია კიბერდანაშაულის მსხვერპლთა დაცვის მექანიზმების შესახებ.

**კიბერდანაშაულს წარმოადგენს** ნებისმიერი მართლსაწინააღმდეგო ქმედება, რომელიც ჩადენილია კომპიუტერული სისტემის გამოყენებით კიბერსივრცეში, რომელიც ხელყოფს კომპიუტერული სისტემის ფუნქციონირებასა და ინფორმაციის დაცულობას.

**კიბერ მეთოდებით ჩადენილი დანაშაულის** შემთხვევაში დანაშაულის ჩამდენი არ ჩადის კიბერდანაშაულს, ჩადის სხვა დანაშაულს (მაგალითად: თაღლითობა, გამოძალვა და ა.შ.) და კომუნიკაციის მეთოდად იყენებს ინტერნეტს (კიბერსივრცეს).

**კომპიუტერული სისტემა** არის ნებისმიერი მექანიზმი ან მექანიზმთან დაკავშირებული ჯგუფი, რომელიც პროგრამის მეშვეობით ამუშავებს მონაცემებს (მაგ. პერსონალური კომპიუტერი, ლეპტოპი, პლანშეტური კოპმიუტერი, მობილური ტელეფონი სმარტფონი და ნებისმიერი მოწყობილობა მიკროპროცესორით).

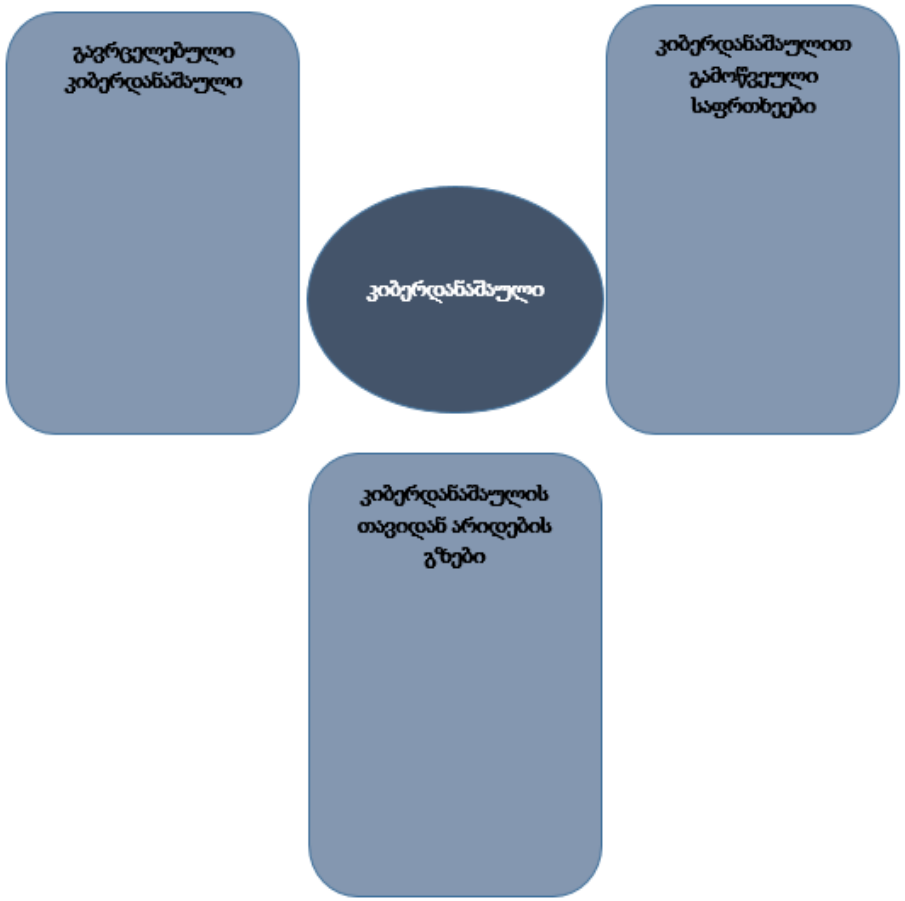
# ინდივიდუალური სამუშაო

***დაფიქრდით:***

- რა ტიპის კიბერდანაშაულია გავრცელებული დღეისათვის საქართველოში ანუ რა ხერხებს მიმართავენ კიბერდანაშაულის ჩადენისათვის (გავრცელებული კიბერდანაშაული)?

- რა საფრთხის წინაშე შეიძლება აღმოჩნდეს კიბერდანაშაულის მსხვერპლი (კიბერდანაშაულით გამოწვეული საფრთხეები)?

- რა გზები არსებობს კიბერდანაშაულის კიბერდანაშაულის თავიდან ასარიდებლად? (კიბერდანაშაულის თავიდან არიდების გზები)?



# რა საფრთხეებს გვიქმნის კიბერდანაშაული?

**შესაძლებელია დამნაშავის ხელში აღმოჩნდეს:**

- პიროვნების პერსონალური მონაცემები;
- პიროვნების პირადი ცხოვრება;

**„პერსონალური მონაცემი** არის ნებისმიერი მონაცემი, რომელიც უკავშირდება იდენტიფიცირებად ან იდენტიფიცირებულ ფიზიკურ პირს.

***მაგალითად:***

სახელი, გვარი;

პირადი ნომერი;

**საბანკო ინფორმაცია;**

ტელეფონის ნომერი;

ელ-ფოსტა;

ინფორმაცია პიროვნების


საკუთრებაში არსებული ქონების შესახებ,

ან სხვა მონაცემი, რომლითაც შესაძლებელია პირის პირდაპირი ან არაპირდაპირი გზით იდენტიფიცირება, კერძოდ, საიდენტიფიკაციო ნომრით, ფიზიკური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლებით“.

**საბანკო ინფორმაციაში** იგულისხმება პიროვნების საკუთრებაში არსებულ საბანკო პლასტიკურ ბარათზე მითითებული ინფორმაცია: სახელი და გვარი, საბანკო პლასტიკური ბარათის ნომერი, მისი მოქმედების ვადა, **CVC** კოდი და მაგნიტური ველი (ბარათის უკანა მხარეს არსებული მუქი ფერის ზოლი), რომელზეც ინფორმაცია დატანილია ელექტრონულად.


**პირადი ცხოვრების ამსახველი ინფორმაცია** შეიძლება იყოს სურათი, აუდიო/ვიდეო ჩანაწერი, მიმოწერა, პირადი ჩანაწერები ან სხვა, რომელიც შეიცავს ადამიანის პირადი ცხოვრების ამსახველ ცნობებს.

# რისთვის ჭირდება დამნაშავეს სხვა ადამიანის პერსონალური მონაცემები და პირადი ცხოვრების ამსახველი ინფორმაცია?

- მიიღოს **ფინანსური სარგებელი;**

- **შანტაჟის ან მუქარის** გზით აიძულოს პიროვნება, განახორციელოს ან თავი შეიკავოს რაიმე ქცევის განხორციელებისგან მისი ნების საწინააღმდეგოდ და დამნაშავის სასარგებლოდ.

**შანტაჟი** - პირის იძულება, შეასრულოს ან არ შეასრულოს რაიმე მოქმედება მისთვის ან მისი ახლობებისათვის სახელის გამტეხი ან სხვა საზიანო ცნობების გახმაურების მუქარით.

**მუქარა** - სიცოცხლის მოსპობის ან ჯამრთელობის დაზიანების ანდა ქონების განადგურების მუქარა, როდესაც იმას, ვისაც ემუქრებიან, გაუჩნდა მუქარის საფუძვლიანი შიში.

# მაგალითი 1.

დამნაშავემ დაინახა, ინტერნეტბანკში შესასვლელად როგორ აკრიფა მისმა თანამშრომელმა კომპიუტერში ავტორიზაციის პარამეტრები - სახელი და პაროლი. დამნაშავემ ეს მონაცემები დაიმახსოვრა, მოგვიანებით თავად გახსნა ინტენეტბანკის გვერდი, აკრიფა მისი თანამშრომლის სახელი და პაროლი, შეაღწია საბანკო ანგარიშზე და იქ არსებული 100 ლარი თავის ანგარიშზე გადარიცხა.

ეს ქმედება არის კიბერდანაშაული თუ კიბერმეთოდებით ჩადენილი დანაშაული?

*ვინაიდან დამნაშავემ უნებართვოდ შეაღწია სხვის კომპიუტერულ სისტემაში (ინტერნეტბანკი არის კომპიუტერული სისტემა) სახეზე გვაქვს კიბერდანაშაული, ხოლო სხვისი ანგარიშიდან თანხის საკუთარ ანგარიშზე გადარიცხვა არის ქურდობა.*

# მაგალითი 2.

დამნაშავეს შექმნილი ჰქონდა ე.წ. ფიშინგ გვერდი (ფიშინგის განმარტება იხ. მომდევნო ქვეთავში), რისი საშუალებითაც ერთ-ერთი სოციალური ქსელის მომხმარებლის ავტორიზაციის პარამეტრები მოიპოვა - კერძოდ, სახელი და პაროლი. ამის შემდეგ, კომპიუტერისა და აღნიშნული ავტორიზაციის პარამეტრების გამოყენებით შეაღწია მოცემული მომხმარებლის სოციალური ქსელის გვერდზე (კომპიუტერული სისტემა) საიდანაც მისი სახელით მიმოწერა აწარმოა მომხმარებლის მეგობრებთან.

ეს ქმედება არის კიბერდანაშაული თუ კიბერმეთოდებით ჩადენილი დანაშაული?

*ვინაიდან დამნაშავემ უნებართვოდ შეაღწია სხვის კომპიუტერულ სისტემაში (სოციალური ქსელის გვერდზე), ადგილი აქვს კიბერდანაშაულს.*

# მაგალითი 3.

დამნაშავე ელექტრონული ფოსტით დაუკავშირდა პიროვნებას მისი კლასელი გიორგის სახელით და მოატყუა, რომ ახლა იმყოფება მეზობელ ქვეყანაში, დაკარგა როგორც ტელეფონი, ასევე პირადი დოკუმენტაცია და გარკვეული პირობების გამო, მას ახალი ელექტრონული ფოსტის გახსნაც მოუწია. თავისი წერილით მან დახმარება და გარკვეული თანხის კონკრეტულ ანგარიშზე გადაგზავნა ითხოვა. ადრესატი წამოეგო ამ სიცრუეს, დაიჯერა, რომ ნამდვილად მისი კლასელი ეკონტაქტებოდა და დამნაშავეს თანხა გადაურიცხა.

ეს ქმედება არის კიბერდანაშაული თუ კიბერმეთოდებით ჩადენილი დანაშაული?

*ვინაიდან დამნაშავეს უნებართვოდ არ შეუღწევია სხვის ელექტრონულ ფოსტაზე და თაღლითურად, თანხის მოტყუებით დაუფლების მიზნით, შექმნა ახალი ელექტრონული ფოსტა, ეს დანაშაული კვალიფიცირდება, როგორც თაღლითობა და დანაშაულის ჩადენის მეთოდად გამოყენებულია კიბერ მეთოდები ანუ ინტერნეტი როგორც კომუნიკაციის საშუალება.*

**ფიშინგი:** ფიშინიგი არის მსხვერპლისთვის ავტორიზაციის პარამეტრების ან მსგავსი ტიპის მონაცემების მოტყუებით მოპოვება, რაც დამნაშავეს შესაძლებლობას აძლევს, უნებართვოდ შეაღწიოს მსხვერპლის პირად გვერდზე.

**ქარდინგი:** ქარდინგი არის საბანკო ბარათების ან სხვა ნებისმიერი საბანკო მონაცემების მოპოვება (ფიშინგით, სკიმერით, ქარდ რიდერით და ა.შ.) და შემდგომ ამ ინფორმაციის გაყიდვა ან გამოყენება ფინანსური სარგებლის მიღების მიზნით.

**ვებგვერდებზე თავდასხმა** გულისხმობს ვებგვერდებზე უნებართვო შეღწევას, რის შემდგომაც დამნაშავეები ეუფლებიან გვერდზე რეგისტრირებულ მომხმარებელთა მონაცემებს ან განათავსებენ სხვადასხვა შინაარსის გამოსახულებებს ტექსტისა თუ ფოტოსურათის სახით.

# შემთხვევების განხილვა - ჯგუფური სამუშაო

*მცირე ჯგუფებში გაეცანით მოცემულ შემთხვევებს და უპასუხეთ ქვემოთ დასმულ კითხვებს:*

- თქვენს მიერ განხილულ შემთხვევაში ადგილი აქვს კიბერდანაშაულს თუ კიბერ მეთოდებით ჩადენილ დანაშაულს?
- კონკრეტულად, რა მეთოდების გამოყენებით მოხდა დანაშაულის ჩადენა?
- რა საფრთხის წინაშე აღმოჩნდა მსხვერპლი?
- საქართველოს სისხლის სამართლის კოდექსის რომელი მუხლით/მუხლებით რეგულირდება ეს დანაშაული?

- *შემთხვევების განხილვის შემდეგ, თითოეულმა ჯგუფმა მოკლედ წარმოადგინეთ თქვენი მოსაზრება ცხრილის დახმარებით.*

# ცხრილი

| შემთხვევის N | დანაშაულის ტიპი (კიბერდანაშაული თუ კიბერ მეთოდებით ჩადენილი დანაშაული?) | გამოკვეთილი დანაშაული | საფრთხე, რომელიც იქმნება მსხვერპლისთვის | სისხლის სამართლის კოდექსის შესაბამისი მუხლი |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# როგორ დავიცვათ თავი კიბერდანაშაულით გამოწვეული საფრთხეებისაგან?

- პერსონალური მონაცემების უსაფრთხოება;
- საბანკო მონაცემების უსაფრთხოება;
- პირადი ცხოვრების ამსახველი ინფორმაციის უსაფრთხოება;
- შანტაჟისა და მუქარისაგან თავის დაცვა

# პერსონალური მონაცემების უსაფრთხოება

- სოციალური ქსელებისა და სხვა ვებგვერდების უსაფრთხოების პარამეტრების გათვალისწინება.
- ორმაგი ავტორიზაციის შესაძლებლობით სარგებლობა.
- სხვადასხვა ვებგვერდზე რეგისტრაციისას სხვადასხვა პაროლის გამოყენება.
- დაცული პაროლის გამოყენება.

დაუცველი პაროლის ნიმუში: gochajojua17


დაცული პაროლის ნიმუში:

ა) **es*aris@chemi^kalami**

ბ) **tiavai** (“თავისუფალი ის არის, ვინც არასოდეს იტყუება”)

გ) **01032005amindi09061963**

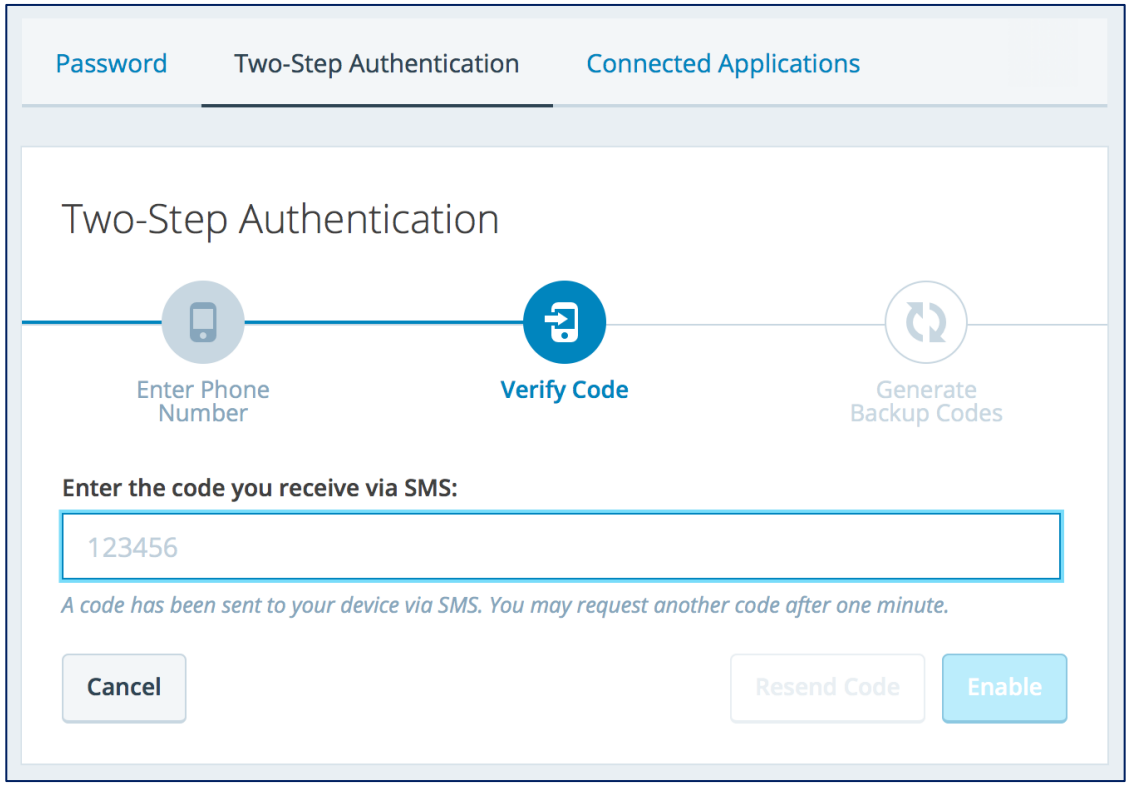
საკუთარი დაბადების თარიღი (პირობითად; 1.03.2005. ), შემდეგ ნებისმიერი სიტყვა, ბოლოს კი, ჯონი დეპის დაბადების თარიღი (9.06.1963.))

# საბანკო მონაცემების უსაფრთხოება

- არ გადავცეთ ჩვენი საბანკო ბარათი ან პლასტიკური ბარათს მონაცემები სხვას.

- თანხის ტერმინალით გადახდისას, საბანკო პლასტიკური ბარათის გამოყენება უნდა მოხდეს მხოლოდ ჩვენი თანდასწრებით.

- გამოვიყენოთ ორმაგი ავტორიზაციის ვებგვერდები.



# პირადი ცხოვრების ამსახველი ინფორმაციის უსაფრთხოება

- დაცულად უნდა შევინახოთ **პირადი მიმოწერა, სურათი, ვიდეო** ან სხვა, რომელიც შეიცავს პირადი ცხოვრების ამსახველ ცნობებს.

- უცნობ ადამიანებთან კონტაქტის დამყარებამდე, საჭიროა გადავამოწმოთ, **რამდენად რეალურია** მათ მიერ მოწოდებული ინფორმაცია, ნამდვილად ის პიროვნებები არიან თუ არა, რომლებადაც თავს ასაღებენ და **დავრწმუნდეთ მათი ქცევის რეალურ მოტივებში.**

# პირადი ცხოვრების ამსახველი ინფორმაციის უსაფრთხოება

**თუ სოციალური ქსელის საშუალებით თქვენთან დამეგობრებას უცნობი ადამიანი ცდილობს:**

- კარგად დაფიქრდით, ვიდრე დაეთანხმებით მის თხოვნას თქვენთან დამეგობრობაზე.

- თუ აღმოაჩენთ, რომ ნამდვილად გაკავშირებთ საერთო ნაცნობები, შეგიძლიათ დაიმეგობროთ, **თუ არა - მაშინ უარი თქვით მასთან კონტაქტზე.**

# შანტაჟისა და მუქარისგან თავის დაცვა

**არ უნდა შევასრულოთ** იმ პირის მითითებები, რომელიც გვიწყობს შანტაჟს ან გვემუქრება, რათა მან არ იგრძნოს ჩვენი სისუსტე და დაუცველობა.

**შანტაჟის ან მუქარის შემთხვევაში აცნობეთ:**

მშობლებს,

მასწავლებელს,

თქვენთვის სანდო სხვა პიროვნებას,

**პირდაპირ პოლიციას.**

**მოაგროვეთ ყველა ფაქტი,** რომელიც მოწმობს დამნაშავის მხრიდან მოწყობილ შანტაჟსა და მუქარაზე.

# კიბერდანაშაულის გამოძიების პროცესში ჩართული სახელმწიფო უწყებები

- **შსს კიბერდანაშაულის სამმართველოს 2 განყოფილება:**

1) საქმის მწარმოებელი გამომძიებლები;
2) გამომძიებლები, რომლებსაც გააჩნიათ სპეციალური ტექნიკური ცოდნა.


- **კიბერტერორიზმის შემთხვევაში,** საქმეს იძიებს სახელმწიფო უსაფრთხოების სამსახური.

# კიბერდანაშაულის მსხვერპლთა დახმარების მექანიზმები

მოქალაქეს შეუძლია დაუკავშირდეს კიბერდანაშაულთან ბრძოლის სამმართველოს ქვემოთ მითითებული ტელეფონის ნომრების საშუალებით:

- **2 41 12 96;**
- **2 41 17 67;**
- **112 - უფასო ცხელი ხაზი 24 საათის განმავლობაში;**
- **ელ–ფოსტა: cybercrime@mia.gov.ge**

გარდა ამისა, მოქალაქეს შეუძლია განცხადებით მიმართოს აღნიშნულ კიბერდანაშაულთან ბრძოლის სამმართველოს, რომლის მისამართია: **ქ.თბილისი გულუას ქ N10.**

# საშინაო დავალება

**1. კითხვებზე პასუხის გაცემა**

ამ დავალების შესრულება ყველა მოსწავლისთვის სავალდებულოა.

*მომდევნო ორი დავალებიდან შესასრულებლად შეგიძლიათ ამოირჩიოთ ერთ-ერთი მათგანი:*

***2. „ორმაგი ჩანაწერების დღიური.“***

**3. "ორი ჭეშმარიტი და ერთი მცდარი დებულება."**

# მადლობა!