Могући ризици

Постоји много начина на који „онлајн криминалци“ могу да вам нанесу штету:

- *Могу да заразе ваш рачунар шпијунским софтвером како би вам украли идентитет*
- *Могу да вас опљачкају, да вам украду идентитет или да вас преваре*
- *Могу да направе збрку у вашем рачунару помоћу „поп-ап“ порука и вируса*
- *Могу да преузму ваш рачунар и да га користе за напад на друге*
- *Могу да вас нападну е-поштом нежељеног или преварног садржаја (spam)*
- *Могу да вас наведу да посетите лажни сајт и дате личне податке*
- *Могу да упадну у вашу бежичну мрежу*
- *Могу да користе ваш налог за слање е-поште и четовање*

Шта може бити угрожено?

- *Ваша приватност*
- *Ваше време*
- *Ваш новац*
- *Ваша репутација*
- *Ваш рачунар*

Република Србија
РАТЕЛ
Републичка агенција за телекомуникације

Вишњићева 8
11000 Београд
www.ratel.rs

Под покровитељством

ACADEMY INA Centre of Excellence

HELLENIC AID

Безбедност на Интернету

Сурфовање по Интернету омогућава крајњем кориснику да се информише, образује, забави, да комуницира и да врши електронске трансакције. Све у свему, употреба Интернета се сматра изузетно важном, а могућности које пружа знатно утичу на квалитет живота.

Ипак, постоје одређени ризици који се односе на употребу Интернета, којих би крајњи корисници требало да буду свесни. На тај начин се активно спречава злоупотреба примене и услуга Интернета.

Како да заштитите свој рачунар

Онлајн криминалци покушавају да нападну ваш рачунар или да би крали од вас или да би нападали друге.
Да бисте их спречили потребна вам је вишеслојна заштита:

- Заштитни софтвер: анти-вирус, анти-спајвер и фајервол или заштитни сет који садржи сва три сигурносна система.
- Ажурирање рачунара, блокирање е-поште нежељеног садржаја (*spam*) и коришћење савремених претраживача.
- Редовно формирање резервних фајлова (*back-up*).
- Такође, добро би било да не користите свој рачунар као администратор (*administrator mode*).
- Коначно, заштитите се од прислушкивања и уљеза применом криптовања у својој бежичној мрежи.

Како да заштитите своју породицу на Интернету

Иако је Интернет драгоцен извор информација и углавном је позитивно место за децу, постоје и реалне опасности. Треба да се упознате са потенцијалним ризицима и да се о томе информишете и ви и ваша породица.

Опасности за децу на Интернету

- Излагање садржајима за одрасле, расистичким садржајима и другим узнемирујућим садржајима.
- Онлајн сусрети са злонамерним и опасним појединцима
- Нарушавање приватности
- Неопрезно коришћење програма за дељење садржаја (*File-Sharing* или *Peer-to-Peer*)

Савети за родитеље

Разговарајте о могућим опасностима Интернета са својом децом

Будите рачунарски писмени

Користите опције родитељског надзора и блокирања софтвера

Задржите приступ налогу за е-пошту свог детета

Обратите пажњу на то шта ваше дете ради на Интренету

Како да заштитите свој идентитет и приватност

Ваш идентитет и ваша репутација су драгоцени. Онлајн „криминалци“ ће на превару покушати да добију личне податке од вас. Циљ је да ви трошите новац, а да они узму новац с вашег рачуна и користе ваше кредитне картице.

Заштитите се од узимања података на превару (*phishing*) и ухођења (*spoofing*):

- Блокирајте нежељену е-пошту (*spam*).
- Користите модерни претраживач који ће вас упозорити на познате лажне вебсајтове.

- Не откривајте своју лозинку и друге личне податке.

Запамтите да на Интернету нема опције „delete“; уколико нешто објавите нећете моћи да контролишете начин на који се ти подаци чувају, копирају или архивирају.

Како избећи преваре код електронских трансакција

Онлајн куповина и банкарство су сигурни и безбедни уколико се придржавате неких једноставних смерница и приступате здраворазумски.

Уколико купујете преко Интернета потражите јасне знакове да је реч о поузданој фирми:

- Да ли постоје и у „стварном“ свету? Да ли можете да пронађете адресу и број телефона?
- Да ли им је вебсајт безбедан? Потражите ‘https://’ и златни катанац.
- Да ли имају јасна правила у вези са приватношћу и враћањем робе?
- Уколико нисте сасвим сигурни, потражите компанију и позовите их како бисте се детаљније информисали.

Уколико користите онлајн сајт за аукције, довољно је неколико једноставних корака како бисте се додатно обезбедили:

- Пре него што почнете, упознајте се са процедуром аукције и правилима сајта.
- Упознајте купца, односно продавца, поставите питања и проверите одговоре.

Осим тога, требало би да научите да препознајете случајеве који би потенцијално могли да доведу до преваре:

- Обећавају велике награде: добитке на лутрији, изгубљена наследства, итд.
- Лажни утисак хитности.
- Необични, сувишни детаљи.
- Захтевају плаћање унапред или давање личних података.