АЕК
MKD-CIRT

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР
НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

САЈБЕР-БЕЗБЕДНОСТ ВО ДОМОТ

ВОДИЧ ЗА РОДИТЕЛИ, ЕДУКАТОРИ И И ДЕЦА

Верзија 1.0
август 2020 година

СОДРЖИНА

ПРЕДГОВОР

Овој водич е направен за да им помогне на родителите, едукаторите и децата за безбедно користење на Интернет.
Според резултатите од Испитување на јавното мислење за примена на мерки за безбедност на Интернет[1], кое го спроведовме во јули 2019 година, корисниците на Интернет во државата се најмногу загрижени за опасностите од кражба на лични податоци, хакирање на профили на социјалните мрежи и измами при купување преку Интернет. Според истото испитување, родителите сметаат дека најважни мерки што треба да се преземат за заштита на децата на Интернет се разговор и едукација на децата, запознаетост на родителите со активностите на децата на Интернет, како и ограничување на времето кое децата го поминуваат на Интернет.
Овој водич содржи совети за сајбер-безбедност наменети за возрасни и деца, како користење на социјалните мрежи, безбедно онлајн-купување, информации за опасносните од лажни вести и потребата за медиумска писменост, како и за заштита при онлајн-играње.
Националниот центар за одговор на компјутерски инциденти MKD-CIRT како дел од Агенцијата за електронски комуникации со овој водич и другите објавени документи и информации, работи активно на подигање на јавната свест за значењето на сајбер-безбедноста. Нашата мисија е да обезбедиме услови за побезбедно користење на Интернет.

Национален центар за одговор
на компјутерски инциденти MKD-CIRT
Агенција за електронски комуникации

https://mkd-cirt.mk

#ЗаштитиСеНаИнтернет

[1] Извештај од испитување на јавно мислење, јули 2019, https://mkd-cirt.mk/2019/07/30/izveshtaj-od-ispituvanje-na-javnoto-mislenje-za-primena-na-merki-za-bezbednost-na-internet/

САЈБЕР БЕЗБЕДНОСТ ВО ДОМОТ

ЗОШТО САЈБЕР-БЕЗБЕДНОСТА Е ВАЖНА?

Несигурните уреди и практики можат да ја загрозат вашата приватност, финансиската добросостојба, па дури и личната безбедност. Несигурните или компромитираните уреди на Интернет можат да шират злонамерен софтвер на уредите на други луѓе.

ПРВО НИВО НА ЗАШТИТА ВО ДОМОТ – РУТЕР

Прво ниво на заштите е рутерот – уредот најчесто поставен од давателот на услугата за Интернет што ја користите во домот. Ако сакате да контролирате на кои веб-страници може да се пристапи од дома, тоа е можно со промена на поставките на вашиот рутер или да побарате помош од давателот на Интернет услугата што ја користите. Информирајте се кај Интернет-провајдерот како да активирате забрани на специфични веб-страници, да поставите контроли на содржини за возрасни и да ограничете користење на Интернет во одреден период од денот.

КОИ СЕ НАЈВАЖНИТЕ ЧЕКОРИ ШТО МОЕТО СЕМЕЈСТВО МОЖЕ ДА ГИ ПРЕЗЕМЕ?

Користете (и не споделувајте) силни лозинки, внимавајте на кои линкови од веб-страници кликнувате, користете софтвери за антивирусна и антиспам заштита, навремено ажурирајте ги оперативните системи и апликациите што ги користите, внимавајте кои апликации ги инсталирате и од кои извори, и не потпаѓајте на измами.

ДАЛИ РИЗИКОТ КАЈ ДЕЦАТА Е ГОЛЕМ?

Да. Младите се многу ранливи на хакерски напади и измами. Тие се најголемите корисници на Интернет и на новите онлајн услуги. Нивната љубопитност може да ги доведе во ризични ситуации во виртуелниот свет.

ШТО Е ДВА-ФАКТОРНА АВТЕНТИКАЦИЈА И ЗА ШТО СЕ КОРИСТИ?

Слично на користењето на кредитни картички, два-факторната автентикација побарува да знаете нешто – на пр. лозинка, но и да имате нешто – како на пр. мобилен телефонски број. Ако се користи два-факторната автентикација, при обид за најава на некоја онлајн услуга од непознат уред, освен лозинката, на мобилниот телефон ќе добиете и код за најава. На тој начин се намалува ризикот некој друг да се најави и да ја користи таа онлајн услуга место вас.

СОВЕТИ ЗА РОДИТЕЛИ

Креирајте уникатни и силни лозинки што можете да ги запомните. Смислете фраза која нема да содржи ваше име, презиме, роденден, но истовремено е лесна да ја запомните. Додадете броеви и специјални знаци. Користете различни лозинки за различни услуги.

ИЗБЕГНУВАЈТЕ „ФИШИНГ“ НАПАДИ

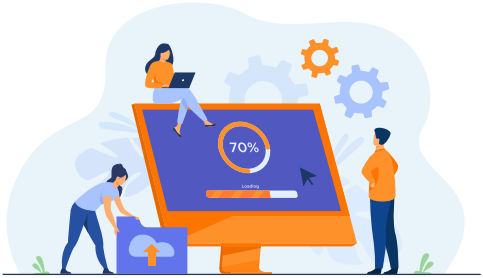
Фишинг е кога ќе добиете порака по е-пошта, на мобилен телефон или преку социјални мрежи, која изгледа како да е испратена од легитимен извор како ваша банка или училиште. Може да содржи додатоци за кои од вас се бара итно да ги отворите и прочитате, или да содржи линк кон веб-страница со барање итно да ги промените корисничкото име или лозинката. Може да содржи измама со цел да ги дадете вашите лични податоци, податоци за кредитни картички и онлајн-плаќања.

ВНИМАВАЈТЕ НА КОИ ЛИНКОВИ КЛИКНУВАТЕ

Преку посета на лажни и малициозни линкови, или со кликнување на линкови од непознати или лажни сајтови, може да иницирате преземање и инсталација на штетен софтвер – малвер (МАЛициозен софтВЕР) кој може да му наштети на уредот преку кој пристапувате на Интернет или кражба на вашите податоци запишани на тој уред. Истото важи и за лажни линкови објавени на социјалните мрежи, преку кои може да се компромитира вашиот профил и во ваше име и без ваше знаење да се испраќаат реклами и други несакани содржини до вашите онлајн-пријатели.

НАВРЕМЕНО АЖУРИРАЊЕ НА СОФТВЕРИ И АПЛИКАЦИИ

Без разлика дали користите компјутер, лаптоп, таблет или мобилен телефон, од голема важност е навремено да се ажурираат оперативните системи и апликациите на уредите преку кои пристапувате на Интернет. Со ажурирањата производителите на софтвери како Microsoft, Google и Apple ги поправаат откриените ранливости во софтверите кои може да бидат искористени и злоупотребени од хакери и криминалци. Секогаш кога е можно вклучете автоматско ажурирање, но по секое ажурирање или надградба, проверете ги поставките за приватност – случајно да не се вратени на основни вредности со кои имате пониско ниво на приватност од саканото.



ВНИМАВАЈТЕ НА ИЗМАМИ

Криминалците често се обидуваат да го искористат интересот за некоја тема или тековни случувања како на пр. коронавирус пандемијата, за да постават лажни веб-страници. Преку нив криминалците се обидуваат да украдат податоци од посетителите, да ги измамат да ги дадат податоците за кредитни картички или лажно нудат продажба на уреди по нереално ниски цени. Проверете ја веродостојноста на веб-страницата со вашето семејство и пријатели. Не правете онлајн-плаќања преку непознати веб-страници, наместо тоа консултирајте се и проверете во вашата банка.

ВНИМАТЕЛНО ПРЕЗЕМАЊЕ (DOWNLOAD)

...на документи и апликации од Интернет. Чест начин за инфицирање на уредите со малвер е преку преземање на апликации и документи од Интернет. Преземајте апликации само од легитимни извори и официјални онлајн пазари како Apple AppStore или GooglePlay. Најпрво прочитајте ги коментарите или барем оценките за апликацијата од други корисници. Истото важи и за софтверите кои се преземаат од веб-страници. Избегнувајте непознати веб-страници и користете само официјални веб-страници на производителите на софтвери.

СОВЕТИ ЗА ДЕЦА НА ИНТЕРНЕТ

Колку што е тешко за возрасните да ја знаат разликата помеѓу легитимна и измамничка веб-страница или услуга, за децата може да биде уште потешко бидејќи тие допрва ги развиваат своите вештини за критичко размислување.

ДЕЦАТА САКААТ ВИДЕА

Малициозните линкови можат да се појават на популарни страници за споделување видео, како YouTube. Прашајте ги вашите деца дали некогаш виделе линкови преку кои се пристапува до несоодветна или нелегална содржина на други страници и прашајте ги што прават кога ќе се сретнат со такви содржини. Рекламите прикажани на веб-страниците исто така можат да ги поврзат децата со содржина што не е соодветна, како и со измами и страници преку кои може да се оддадат чувствителни информации.

ДЕЦАТА ЧЕСТО КОРИСТАТ СЕМЕЈНИ КОМПЈУТЕРИ

Можеби мислите дека децата не се подложни на финансиски криминал бидејќи немаат кредитни картички, но ако децата користат ист компјутер или уред со родители, нивните активности на Интернет можат да влијаат врз сите корисници на тој уред и активностите како купување преку Интернет, онлајн банкарство или користење на уредот за работа. Родителите и возрасните лице треба да се свесни дека ако децата ја проверат историјата на прелистувачот, можат да бидат изложени на страници што нивните родители ги посетуваат на семејниот компјутер.

ДОБРА ПРАКСА ЗА ЛОЗИНКИ

Научете ги вашите деца да не ги споделуваат лозинките со нивните пријатели, и секогаш да се одјавуваат од онлајн услугите што ги користат, особено од јавни места и уреди, како на пример на училиште или во библиотеки. Прелистувачите (на пр. Internet Explorer, Google Chrome и други) користат колачиња (cookies) со кои привремено се зачувуваат лозинките и активностите од претходните корисници на прелистувачот и комппјутерот. Секогаш кога е можно преку опциите на прелистувачот треба да се избира т.н. приватен режим на работа (или „инкогнито“), и не заборавајте да ги избришете колачињата и историјата на прелистувачот.

ОНЛАЈН ИГРИ

Советите наведени подолу имаат за цел да ве заштитат вас и вашите лични податоци при онлајн играње. Без разлика дали користите компјутер, конзола, телефон или таблет, овие совети ќе ви помогнат да не бидете жртва на сајбер криминалци.

БЕЗБЕДНОСТ НА УРЕДИТЕ ЗА ОНЛАЈН ИГРАЊЕ

Поголемиот дел од сајбер нападите ги искористуваат јавно познатите слабости во уредите и софтверите. Нивно навремено ажурирање ќе помогне да се спречат овие напади да бидат успешни. Најлесен начин за навремено ажурирање на уредите и апликациите е да вклучите автоматско ажурирање, секогаш кога тоа е можно. Кога е можно, додадете дополнителен слој на одбрана на вашите уреди преку инсталација на антивирусен софтвер што исто треба навремено да се ажурира.

ЗАШТИТА НА КОРИСНИЧКИ СМЕТКИ ЗА ОНЛАЈН ИГРАЊЕ

Вашите сметки за онлајн игри треба да ги заштитите со користење на силни лозинки и иста лозинка да не се користи за повеќе сметки и онлајн услуги. Секогаш кога е можно вклучете два-факторна автентикација со што ќе додадете дополнителен безбедносен слој и ќе спречите некој хакер или криминалец да пристапи до вашата сметка.

ЗАШТИТА НА ПРИВАТНОСТ

Обидете се да информациите што ги споделувате на Интернет да бидат минимални. Користете ги поставките за приватност за да осигурите дека вашите лични податоци не се видливи за другите играчи и не споделувајте лични податоци со нив. Кога се ослободувате од стари конзоли, компјутери, таблети и телефони, проверете дали претходно сте ги избришале сите лични податоци и детали за кориснички сметки од овие уреди.

КОРИСТЕЊЕ НА ОФИЦИЈАЛНИ ИЗВОРИ И ОНЛАЈН ПРОДАВНИЦИ

Секогаш треба да го проверите изворот на сè што инсталирате. Најлесен начин да го направите ова е да користите официјални извори и продавници за игри. Сајбер криминалците се обидуваат да ги заобиколат безбедносните мерки во игрите, со убедување да направите нешто надвор од самата игра. На пример, играч што не го знаете може да предложи да инсталирате „надградба“ и да ви прати линк за преземање. Предлогот може да дојде и во форма на лажна порака по е-пошта, со ветување за бесплатно користење на некоја игра или надградба. Преку користење на официјалните извори за целиот ваш софтвер, помала е веројатноста случајно да инсталирате малвер на вашиот компјутер, таблет или друг уред.

СОВЕТИ ЗА РОДИТЕЛИ И ДЕЦА

- Дознајте кои игри сакаат да ги играат децата. Заинтересирајте се за игрите што ги играат вашите деца, како се играат тие игри и зошто тие уживаат во играњето.

- Дознајте со кого играат. Прашајте со кого играат преку Интернет, со кого се среќаваат и разговараат онлајн, и разговарајте за тоа каков јазик се користи. Осигурете се дека вашето дете знае како да пријави секоја нелагодност од овие разговори што може да биде знак за онлајн малтретирање и да предизвика антисоцијално однесување

- Исклучете ја врската со Интернет секогаш кога е можно. За помалите деца, користете ги поставките на уредите за т.н. „airplane“ – авион-режим на работа на вашиот таблет или паметен телефон. На тој начин, децата можат да играат „офлајн“, т.е. да не се поврзани на Интернет, без да направат случајни онлајн купувања или да се поврзат со непознати лица.

- Изберете игри соодветни на возраста на детето. Користете ги оценките за PEGI и рејтингот на продавниците за апликации за да се осигурате дека вашето дете игра игри соодветно на возраста. Помогнете му на детето да разбере зошто некои игри се дозволени, а други не.

- Договорете дигитални граници. Играњето може да биде многу зависно, затоа договорете ги границите за тоа кои содржини и сервиси на Интернет можат да ги користат, колку долго ќе им биде дозволено на децата да играат и со кого им е дозволено да играат преку Интернет. Потсетете ги дека луѓето понекогаш лажно се претставуваат и дека криминалци се кријат зад лажни имиња, слики и профили.

СОЦИЈАЛНИ МРЕЖИ

Без разлика дали станува збор за Фејсбук, Твитер или Инстаграм, пред да се отвори корисничка сметка за вашето дете, најпрво треба да се запознаете со контролите за приватност на таа друштвена мрежа.

ФЕЈСБУК / FACEBOOK

Малку луѓе не слушнале за Фејсбук, најголемата социјална мрежа во светот. Денес, на платформата се објавуваат фотографии од деца уште пред да прозборат, и иако Фејсбук побарува од своите корисници да имаат најмалку 13 години кога ќе се зачленат, родителите честопати го инорираат ова правило. Фејсбук е одлично место за одржување на контакти со пријателите и семејството, но платформата може да биде злоупотребена и за сајбер-малтретирање (cyberbullying), за собирање на лични податоци и објава на лажни вести.

Ако вашето дете сака сметка на Фејсбук, добро да се договорите дека ќе имате целосен пристап до сметката и пораките на детето, се додека не оцените дека детето е доволно зрело. Треба да воспоставите баланс меѓу грижата на родителот и приватноста на детето како индивидуа, и на тој начин да помогнете во неговата заштита од сајбер-малтретирање и несоодветни содржини. Фејсбук има посебна

апликација Messenger Kids за корисници на возраст под 13 години.

ТВИТЕР/TWITTER

Твитер е платформа за микроблогирање која се користи за објавување јавни пораки - твитови, но и за споделување видеа и слики. Може да биде важна алатка за комуникација со училиштата, деловните субјекти и организациите, како и за добивање на информации за активности на други корисници на Твитер што ги следиме. Но платформата може да биде и место за злоупотреба и тролање. Откако ќе се отвори корисничка сметка, главните ограничувања и контроли кои треба да ги знаете и поставите се наоѓаат во менито “Settings and privacy / Прилагодувања и приватност”.

YOUTUBE

За да ја чувате вашата сметка на Youtube и Google безбедна, креирана е листа за проверки што ќе ви помогне да ги обезбедите вашиот компјутер, прелистувачот, Gmail и сметката на Google. Ве охрабруваме да ја поминете целата листа за проверка, но сакаме да ги потенцирате следниве чекори што можат да ви помогнат да го одржите вашиот канал на YouTube безбеден.

- Додајте телефонски број за обновување на пристап до корисничката сметка и секундарна адреса за е-пошта на вашата сметка на Google. Немањето телефонски број и безбедна е-пошта значи дека на вашата сметка може да пристапи некој што ја дознал вашата лозинка.

- Чувајте ги вашите информации за обновување на сметката безбедни и ажурирани.

- Создадете единствена, силна лозинка за вашата сметка на Google (и не ги користете истите корисничко име и лозинка за најава на други страници).

- Ако сметате дека вашата сметка е загрозена, можете да ја пријавите овде https://support.google.com/youtube/contact/compromised_account

YouTube Kids е создаден за да биде забавно, семејно-ориентирано место за деца и семејства. Апликацијата YouTube Kids вклучува и популарни видеа за деца и разновидна нова содржина, испорачана на начин што е лесен за употреба за деца од која било возраст. YouTube Kinds е достапен на следниот линк: https://www.youtube.com/kids/

ТИКТОК

Што е TikTok? TikTok е апликација која им дава можност на корисниците да создаваат кратки видеа и да ги споделуваат со пријателите, семејството, и целиот свет. Апликацијата е особено популарна кај тинејџерите и младите. Оваа апликација овозможува комбинирање на видео, музика и графика. TikTok работи на Apple и Android телефони и таблети. Според информациите објавени на официјалните пазари за апликации Apple App Store и Google Play Store, апликацијата е наменета за возраст од 13 или повеќе години.

Постои верзија на TikTok за деца под 13 години, за чие користење е неоходна согласност од родителите и која спречува јавно објавување на содржини. 13+

Дали видеата поставени на TikTok се приватни или јавно достапни? Корисничките сметки на TikTok се јавни, што овозможува секој да го гледа профилот на корисникот и неговите објавени видеа. Корисниците имаат можност да го променат својот профил во приватен. Ова им овозможува на корисниците да одобрат или одбијат следбеници и во тој случај само вашите одобрени следбеници можат да ги гледаат вашите видеа.

Како безбедно да се користи TikTok? Започнете со разговор со своето дете за тоа како се користи TikTok. Бидете сигурни дека децата разбираат дека видеата и коментарите што ги објавуваат влијаат на нивниот углед и дека тие никогаш не треба да објавуваат ништо што ја загрозува нивната приватност и безбедност. Бидете сигурни дека вашето дете знае како да блокира секој што му се заканува или го малтретира онлајн преку оваа апликација, или ако децата не сакаат таа личност да ја види нивната содржина или да ги коментира нивните видеа.

TikTok исто така им овозможува на корисниците (или нивните родители) можност да филтрираат содржини наменети за возрасна публика со овозможување на т.н. Ограничен режим. Родителите

можат да ги постават овие ограничувања само ако имаат пристап до уредот, корисничкото име и лозинката на нивните деца.

INSTAGRAM

Што е Instagram? Instagram е апликација која се користи за споделување фотографии, видеа и пораки. Без разлика дали е преку Stories, Feed, Live, IGTV или Direct, тинејџерите користат Instagram за да прослават активности, да споделуваат секојдневни моменти, да останат во контакт со пријателите и семејството, да градат мрежа на пријатели и да запознаваат други луѓе со кои делат слични интереси. Оваа апликација е достапна за компјутери и Apple и Android мобилни уреди.

Минимална возраст? Минималната возраст за користење на Instagram е 13 години, што е наведено при регистрација на нов корисник. Instagram не бара од корисниците да ја прецизираат нивната возраст и има многу помали деца кои ја користат услугата, честопати со дозвола на нивните родители. Инстаграм ќе ги избрише сметките на малолетници доколку некој пријави и не може да потврди дека корисникот има најмалку 13 години.

Кои се ризиците? Главни ризици се слични како и за останатите социјални медиуми: однесување меѓу врсници, несоодветни фотографии или видеа што можат да му наштетат на угледот на тинејџерот или да привлечат погрешен вид на внимание, злоупотреба и приватност. Ризик е што луѓето кои децата не ги познаваат можат директно да пристапат до нивните јавни профили и објавени содржини.

Заштита на приватност и безбедност на Instagram? Започнете со тоа што корисничката сметка ќе ја направите приватна. На тој начин само луѓето кои ги одобрувате ќе може да ги видат вашите слики, видеа и мислења. Исто така, Instagram има алатки за блокирање на луѓе и пријава на несоодветни содржини и коментари, како и за ограничување на времето што го поминувате во активно користење на апликацијата.

БЕЗБЕДНО ОНЛАЈН КУПУВАЊЕ

НЕ ДОЗВОЛУВАЈТЕ ДА ВЕ ИЗЛАЖАТ!

Ако звучи премногу добро за да биде вистинито, најверојатно не е вистинито. Ако цената е МНОГУ пониска од огласени цени на други места и кај други продавачи, може да станува збор за измама или предметот што сакате да го купите онлајн да е претходно користен или неисправен. Проверете за да знаете што добивате.

ВРАЌАЊЕ НА КУПЕН ПРОИЗВОД.

Бидете сигурни дека ја разбирате политиката за враќање, вклучувајќи ги и роковите и дали ќе мора да плаќате за враќањето кое може да биде скапо за големи и тешки производи. Бидете сигурни дека ја знаете целосната цена на производот, вклучувајќи испорака и други давачки. Размислете за купување во онлајн продавница која има физичка локација во ваша близина, што ви овозможува бесплатно враќање на предметите. Повеќе информации ќе најдете на веб-страницата на Организација на потрошувачи на https://opm.org.mk/

КУПУВАЈТЕ САМО ОД ПОЗНАТИ ИЗВОРИ

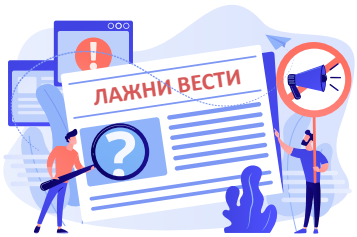
Купувајте преку Интернет само од реномирани продавачи. Кога се сомневате, распрашајте се и истражете за нив на Интернет. Прочитајте ги коментарите (не само оние објавени на нивната страница) и побарајте објави за продавачот со вклучен збор „измама“ (fraud, scam). Сите продавачи ќе имаат неколку лоши коментари, затоа погледнете повеќе коментари и рецензии за да добиете целосен впечаток. Бидете особено внимателни пред да купувате кај непознати продавачи кои ви праќаат реклами и понуди преку е-пошта и пораки.

БЕЗБЕДНО ПЛАЌАЊЕ

Никогаш не испраќајте пари и не користете сервиси за пренос на пари. Ако можете користете кредитни или дебитни картички, или познати сервиси за онлајн плаќања како што се Paypal, GooglePay или ApplePay. Пред да почнете со онлајн плаќања, информирајте се во вашата банка за начинот на заштита од измама.

МЕДИУМСКА ПИСМЕНОСТ И ЛАЖНИ ВЕСТИ

Што е медиумска писменост и зошто е важна? Накратко, медиумската писменост критичко размислување за информациите што ги конзумирате и создавате. Вклучува способност да се разликува факт од мислење или лажни информации и да се разбере како медиумите понекогаш можат да се користат за да се убедат луѓето. Постои ризик децата да не прават разлика помеѓу реклами и вистински вести. Како родители и воспитувачи, ваша обврска е да им помогнете на децата да станат информирани корисници и создавачи на информации и содржини.



Што се лажни вести и зошто луѓето ги создаваат? Лажни вести се сите информации што се целосно или во голема мера лажни или погрешни. Мотивациите за создавање лажни вести вклучуваат финансиска добивка со тоа што луѓето ќе кликнат на страници и со тоа ќе бидат изложени на рекламирање или убедување за да преземат некоја активност, да купат некој производ или да поддржуваат или да се спротивстават на кауза или политички кандидати и опции. Некои луѓе објавуваат лажни вести само за да ги измамат луѓето или како шега. Искрени грешки се случуваат и тие не се лажни вести. Но, оние што објавуваат или

кажуваат нешто за што подоцна откриваат дека се невистинити, имаат обврска да ја поправат објавата и направат исправка на информацијата.

Повеќе информации за медиумската писменост ќе најдете на следниот линк https://mediumskapismenost.mk.

ГОВОР НА ОМРАЗА И НАСИЛЕН ЕКСТРЕМИЗАМ

ШТО Е ГОВОР НА ОМРАЗА?

Говорот на омраза е повеќе од само груби зборови. Може да биде каков било облик на изразување наменет да понижува или да поттикнува омраза против група на луѓе. Може да се појави во реалниот живот и преку Интернет. Може да се извршува со употреба на зборови, симболи, слики, или видеа. Во принцип, говорот на омраза е насочен кон некоја личност или група заради карактеристиките што се тесно поврзани со нивниот идентитет, како раса, боја, религија, етничка припадност, пол, сексуална ориентација или попреченост.

ШТО Е НАСИЛЕН ЕКСТРЕМИЗАМ?

Екстремизмот е гласно или активно спротивставување на основните општествени вредности, вклучувајќи демократија, владеење на правото, индивидуална слобода и взаемно почитување и толеранција на различни вери и верувања.

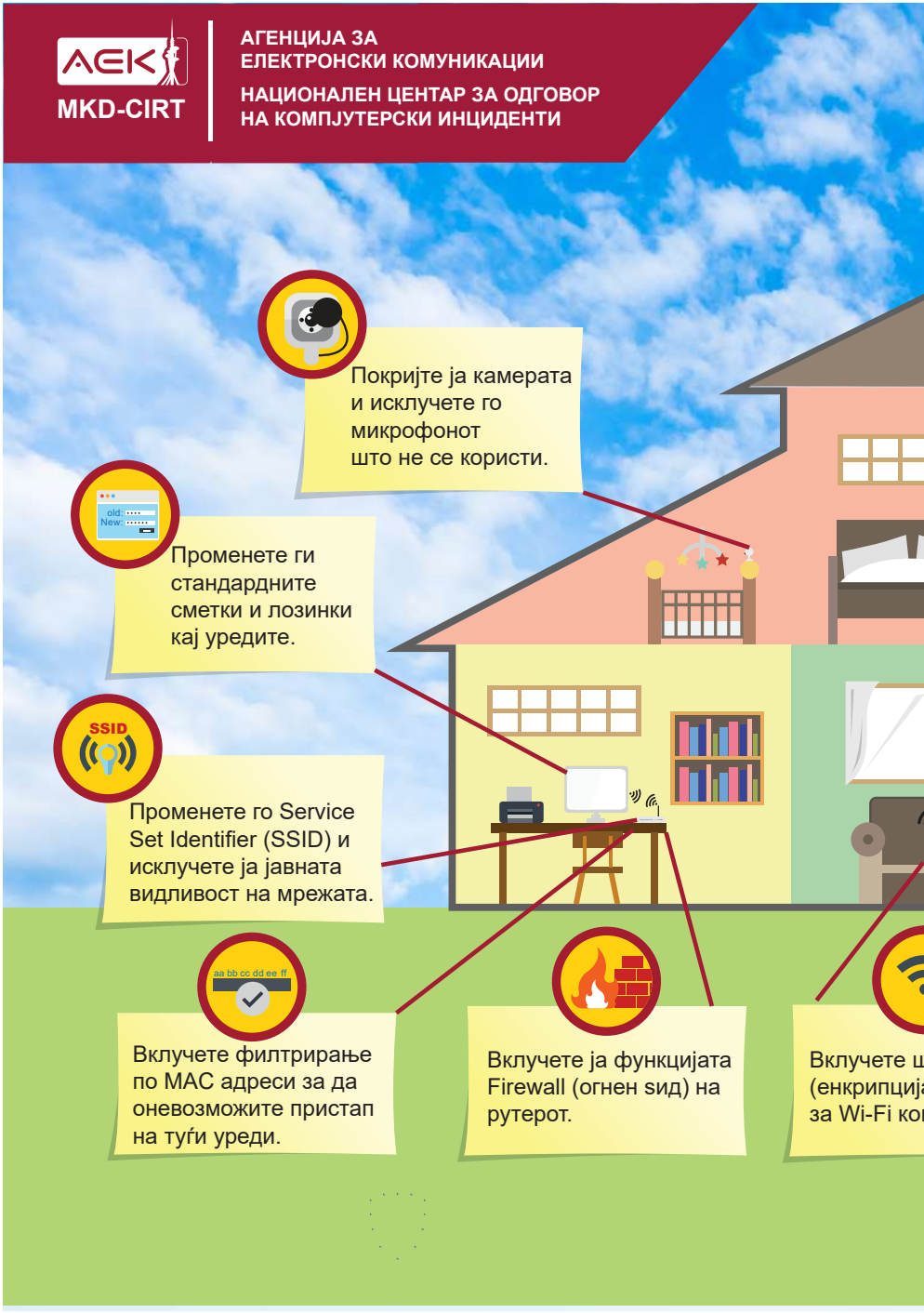
Постојат обиди да се радикализираат ранливите деца и млади, со цел тие да развиваат екстремни ставови. Овие ставови се однесуваат на погледи со кои се оправдува политичкото, религиозното, сексистичкото или расистичкото насилство, или со кои луѓето се насочуваат кон ригидна и тесна идеологија која е нетолерантна кон различностите и ги остава подложни на идна радикализација.

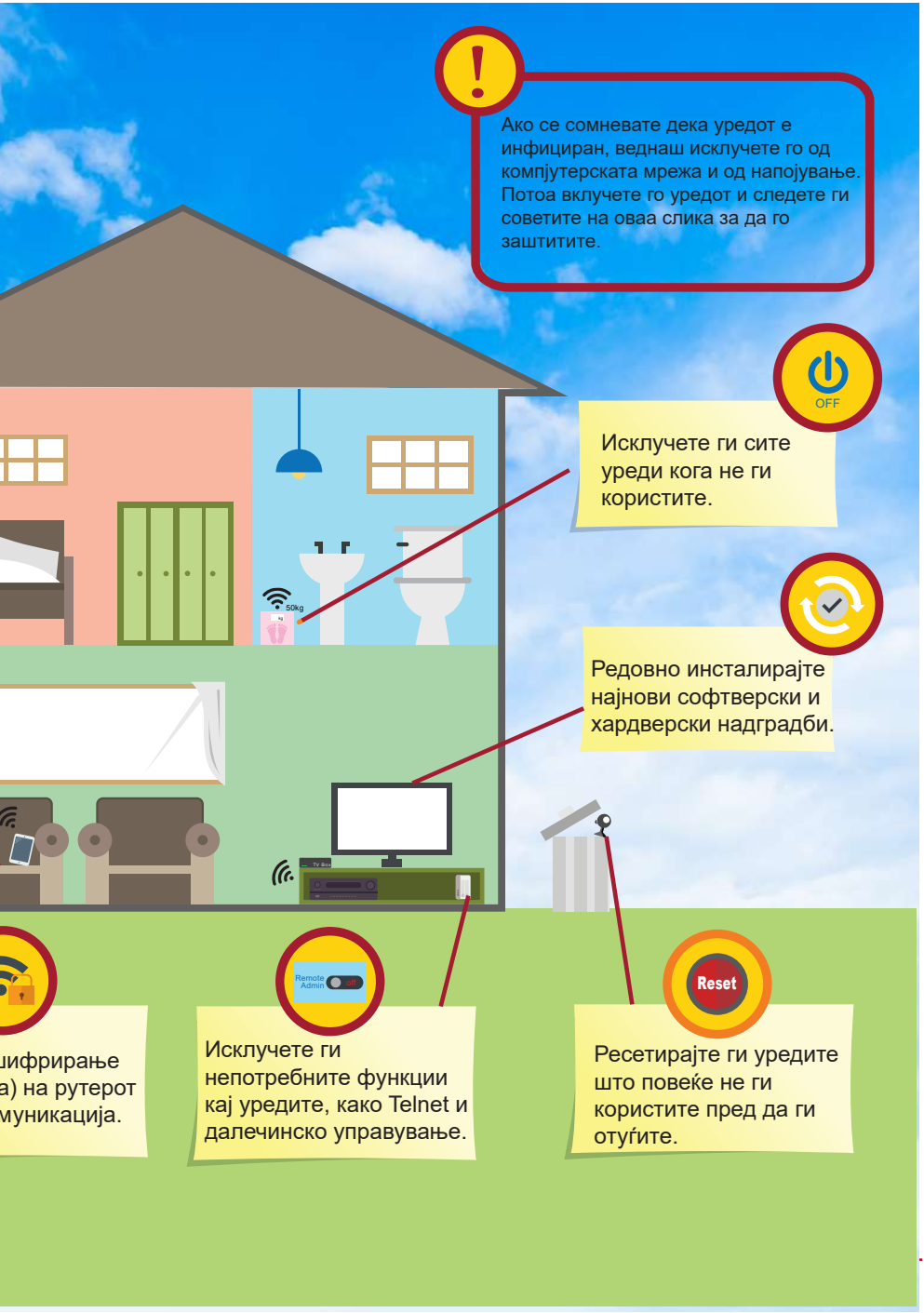
РИЗИЦИ

Децата и младите можат да бидат вовлечени во насилство или можат да бидат изложени на пораките на екстремистичките групи на многу начини, преку влијанието на членовите на семејството или пријателите, или преку директен контакт со екстремистичките групи и организации. Сè поважно е изложувањето преку Интернет, преку социјалните мрежи и веб-страници. Заштита и мерки што треба да се преземат при Интернет радикализација. Родителите се клучни во сузбивање на радикалните погледи и екстремистичкото однесување кај децата. Разговарајте со вашето дете за безбедноста на Интернет, објаснете ги опасностите и проверете дали нивните сметки на социјални мрежи се безбедни. Инсталирајте родителските контроли за да можете да следите кон што пристапуваат на интернет.

Корисни предлози за да го зачувате вашето дете безбедно:

- Зборувајте со вашето дете за она што тие го прават преку Интернет
- Побарајте од нив да ви покажат некои од нивните омилени страници
- Покажете интерес за тоа кои се нивните пријатели на Интернет
- Прашајте ги како тие одлучуваат со кого да бидат пријатели
- Станете онлајн-пријатели со вашите деца на социјалните мрежи што ги користат. На тој начин ќе имате увид во нивните објави како поставени слики.
- Договорете се за прифатливо време за користење на Интернет и кои страници е прифатливо да ги посетуваат
- Размислете за инсталирање на родителски контроли на нивните уреди
- Поставете го прашањето што е „несоодветна содржина“. Дали децата виделе нешто сомнително или невообичаено?
- Бидете сигурни дека децата знаат како да пријават злоупотреба преку Интернет.


MKD-CIRT
АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ
НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ
Покријте ја камерата и исклучете го микрофонот што не се користи.
old:
New:
Променете ги стандардните сметки и лозинки кај уредите.
SSID
Променете го Service Set Identifier (SSID) и исклучете ја јавната видливост на мрежата.
aa bb cc dd ee ff
Вклучете филтрирање по MAC адреси за да оневозможите пристап на туѓи уреди.
Вклучете ја функцијата Firewall (огнен ѕид) на рутерот.
Вклучете ш
(енкрипција
за Wi-Fi ко


Ако се сомневате дека уредот е инфициран, веднаш исклучете го од компјутерската мрежа и од напојување. Потоа вклучете го уредот и следете ги советите на оваа слика за да го заштитите.
OFF
Исклучете ги сите уреди кога не ги користите.
Редовно инсталирајте најнови софтверски и хардверски надградби.
50kg
Remote Admin
off
Reset
Исклучете ги непотребните функции кај уредите, како Telnet и далечинско управување.
Ресетирајте ги уредите што повеќе не ги користите пред да ги отуѓите.
шифрирање
а) на рутерот
муникација.

САЈБЕР-БЕЗБЕДНОСТ ВО ДОМОТ
Водич за родители, едукатори и деца

ВО ОВОЈ ВОДИЧ ЌЕ НАЈДЕТЕ СОВЕТИ ЗА

- САЈБЕР-БЕЗБЕДНОСТ ВО ДОМОТ
- БЕЗБЕДНО ОНЛАЈН-ИГРАЊЕ
- МЕДИУМСКА ПИСМЕНОСТ И ЛАЖНИ ВЕСТИ
- ПРЕПОЗНАВАЊЕ И ЗАШТИТА ОД ГОВОР НА ОМРАЗА И НАСИЛЕН ЕКСТРЕМИЗАМ
- БЕЗБЕДНО ОНЛАЈН КУПУВАЊЕ

Повеќе информации и совети за сајбер-безбедност ќе најдете на веб-страницата на Националниот центар за одговор на компјутерски инциденти MKD-CIRT https://mkd-cirt.mk

Прашања и пријави на инциденти испраќајте на info@mkd-cirt.mk или 02/3091232

#BezbednoNaInternet