МЕПСО

ПРИРАЧНИК

Прирачник за сајбер безбедност

Свест, препознавање на закани и заштита во дигиталниот свет

Придружен материјал за обуката:
„Зголемување на свест за сајбер безбедност"

Документ бр. МЕПСО-ПРИ-САЈ-003 · Класификација: Интерна употреба
Сектор за информатичка и сајбер безбедност · МЕПСО АД Скопје

Содржина

1. Вовед

Живееме во свет каде речиси сè е поврзано — работата, комуникацијата, финансиите. Оваа поврзаност носи огромни придобивки, но и нови ризици кои сите треба да ги разбереме.

Сајбер безбедноста не е само задача на техничките експерти. Секој од нас, преку своите секојдневни дигитални навики, придонесува кон безбедноста или ранливоста на организацијата. Овој прирачник ќе ви даде основно разбирање на заканите и практични навики за заштита.

Не треба да бидете технички експерт за да бидете безбедни. Треба само да развиете свест, здрав скептицизам и неколку добри навики. Тоа е доволно за да ги избегнете најголемиот дел од заканите.

Зошто е важно. Сајбер нападите не бираат — можат да погодат секого. Но информираниот и внимателен корисник е многу потешка мета. Знаењето е вашата најдобра одбрана.

2. Што е сајбер безбедност

Сајбер безбедноста е практика на заштита на системи, мрежи, уреди и податоци од дигитални напади. Целта е да се обезбеди доверливост, интегритет и достапност на информациите.

2.1 Зошто е важна за секого

- Штити ги вашите лични и работни податоци;
- Спречува финансиски загуби и кражба на идентитет;
- Обезбедува непрекинато работење на организацијата;
- Заштитува ја критичната инфраструктура од која зависи општеството.

2.2 Човечкиот фактор

Голем дел од успешните напади ја искористуваат човечката природа — љубопитност, доверба, страв, желба да се помогне. Технологијата може да заштити многу, но крајната одлука често е ваша.

Факт. Најголемиот дел од безбедносните инциденти вклучуваат човечка грешка. Токму затоа вашата свест и внимание се клучни.

3. Пејзаж на современите закани

Заканите се разновидни и постојано еволуираат. Еве ги најчестите:

Закана	Опис
Малициозен софтвер	Вируси, црви, тројанци што штетат на системите
Ransomware	Заклучува податоци и бара откуп
Phishing	Измама преку лажни пораки
Социјален инженеринг	Манипулација на луѓе за откривање информации
Кражба на идентитет	Злоупотреба на лични податоци
Напади на лозинки	Обиди за погодување или кражба на лозинки

4. Малициозен софтвер

Малициозен софтвер (malware) е секој програм создаден да наштети, украде податоци или неовластено пристапи до систем.

4.1 Видови

Вид	Однесување
Вирус	Се прикачува на датотеки и се шири
Црв	Се шири самостојно низ мрежи
Тројанец	Се маскира како легитимен програм
Шпионски софтвер	Тајно собира информации
Рекламен софтвер	Прикажува нежелени реклами

4.2 Како се шири

- ✓ Заразени прилози во е-пошта
- ✓ Малициозни линкови и веб-страници
- ✓ Заразени USB уреди
- ✓ Пиратски или неодобрен софтвер
- ✓ Неажурирани системи со безбедносни пропусти

4.3 Заштита

- ✓ Одржувајте активен и ажуриран антивирус
- ✓ Редовно ажурирајте го оперативниот систем
- ✓ Не инсталирајте неодобрен софтвер
- ✓ Внимавајте со прилози и линкови
- ✓ Не приклучувајте непознати USB уреди

5. Ransomware — заклучување за откуп

Ransomware е особено опасен вид малициозен софтвер што ги шифрира вашите податоци и бара откуп за да ги отклучи. Може да го парализира целото работење.

5.1 Како функционира

По инфекцијата, ransomware ги заклучува датотеките и прикажува порака со барање за плаќање, најчесто во криптовалута, во замена за клучот за отклучување.

> **Важно.** Плаќањето на откуп не гарантира враќање на податоците и го поттикнува криминалот. Најдобрата заштита е превенцијата и редовните резервни копии.

5.2 Заштита

- ✓ Правете редовни резервни копии на важните податоци
- ✓ Не отворајте сомнителни прилози или линкови
- ✓ Одржувајте ги системите ажурирани

- ✓ Пријавете веднаш ако забележите необично шифрирање на датотеки

6. Социјален инженеринг

Социјалниот инженеринг е манипулација на луѓе за да откријат доверливи информации или да преземат дејства што ја загрозуваат безбедноста. Наместо да напаѓаат технологија, напаѓачите ја напаѓаат човечката природа.

6.1 Чести техники

Техника	Опис
Претставување	Преправање дека е доверлива личност или институција
Итност	Создавање притисок за брза, непромислена реакција
Авторитет	Претставување како надреден или власт
Помош	Искористување на желбата да се помогне
Љубопитност	Мамки што ја предизвикуваат љубопитноста

Одбрана. Здравиот скептицизам е клучен. Ако нешто изгледа итно, необично или премногу добро за да биде вистина — застанете и проверете преку независен канал.

7. Безбедност на лозинки и сметки

Лозинките се клучевите на вашиот дигитален живот. Нивната заштита е основа на сајбер безбедноста.

- ✓ Користете долги лозинки (најмалку 12 знаци)
- ✓ Комбинирајте букви, бројки и симболи
- ✓ Уникатна лозинка за секоја сметка
- ✓ Користете менаџер за лозинки
- ✓ Вклучете двофакторна автентикација секаде каде е достапна
- ✓ Никогаш не споделувајте лозинки

Совет. Двофакторната автентикација е една од најефикасните заштити. Дури и ако лозинката биде компромитирана, вториот фактор ја спречува неовластената најава.

8. Безбедно прелистување на интернет

- ✓ Проверувајте дали адресата започнува со „https" за чувствителни страници
- ✓ Внимавајте на сомнителни или непознати веб-страници
- ✓ Не преземајте датотеки од недоверливи извори
- ✓ Внимавајте на лажни реклами и pop-up прозорци
- ✓ Одржувајте го прелистувачот ажуриран

9. Мобилни уреди и безбедност

Паметните телефони и таблети содржат многу чувствителни информации и се често мета.

- ✓ Заклучувајте го уредот со ПИН, лозинка или биометрија
- ✓ Инсталирајте апликации само од официјални продавници
- ✓ Внимавајте на дозволите што ги бараат апликациите
- ✓ Одржувајте го оперативниот систем ажуриран
- ✓ Не оставајте го уредот без надзор
- ✓ Овозможете далечинско бришење во случај на загуба

10. Безбедност на јавни мрежи

Јавниот WiFi (кафулиња, аеродроми, хотели) е погоден, но носи ризици. Напаѓачите можат да прислушкуваат сообраќај на незаштитени мрежи.

Правило. Не пристапувајте до чувствителни системи или не внесувајте лозинки преку јавен WiFi без VPN. Секогаш користете VPN за безбедна врска.

- ✓ Користете VPN на јавни мрежи
- ✓ Избегнувајте чувствителни трансакции на јавен WiFi
- ✓ Исклучете автоматско поврзување со отворени мрежи
- ✓ Проверете го името на мрежата — напаѓачите создаваат лажни

11. Заштита на приватноста

- ✓ Внимавајте што споделувате на социјални мрежи
- ✓ Прегледајте ги поставките за приватност
- ✓ Не објавувајте чувствителни лични или работни информации
- ✓ Внимавајте — информациите што ги објавувате можат да се искористат против вас

12. Резервни копии и опоравување

Резервните копии се вашата сигурносна мрежа. Ако податоците се изгубат поради напад, дефект или грешка, копијата овозможува враќање.

- ✓ Правете редовни резервни копии на важните податоци
- ✓ Чувајте копии на безбедно, одвоено место
- ✓ Проверувајте дека копиите функционираат
- ✓ Следете ја препораката на ИТ Секторот за начинот на архивирање

Практични сценарија

Сценарио 1: Итен повик за „техничка поддршка"

Ве вика некој што тврди дека е од техничка поддршка и дека вашиот компјутер е заразен. Бара да инсталирате програм за далечински пристап за да го „поправи".

> **Правилна реакција:** Не инсталирате ништо и не давате пристап. Легитимната поддршка не ве вика неочекувано вака. Прекинувате и пријавувате на вистинскиот ИТ Сектор.

Сценарио 2: Бесплатен подарок

Добивате известување дека сте добиле награда и треба да внесете лични податоци за да ја подигнете.

> **Правилна реакција:** Игнорирате. Ако нешто е премногу добро за да биде вистина, најверојатно е измама. Не внесувате никакви податоци.

Сценарио 3: Сомнителна апликација

Пронаоѓате апликација што ветува корисна функција, но бара пристап до контакти, пораки и локација иако тоа не е потребно за нејзината намена.

> **Правилна реакција:** Не ја инсталирате. Прекумерните дозволи се знак за сомнителна апликација. Инсталирате само од официјални извори.

Најчесто поставувани прашања

Дали антивирусот ме штити целосно?

> Не. Антивирусот е важен слој, но не е доволен сам. Вашата внимателност, ажурираните системи и добрите навики се подеднакво важни.

Што е најважно за сајбер безбедност?

> Свеста. Повеќето напади бараат вашето учество (клик, внесување податоци). Внимателниот корисник ги избегнува најголемиот дел од заканите.

Колку често треба да менувам лозинка?

> Кога има сомнеж за компромис, и за критични сметки периодично. Поважно од честото менување е лозинката да биде силна, уникатна и заштитена со 2FA.

Дали е безбедно да користам јавни компјутери?

> Со голема претпазливост. Не внесувајте лозинки за чувствителни сметки, секогаш одјавувајте се, и не оставајте лични податоци. По можност, избегнувајте ги за важни работи.

Што ако мислам дека сум заразен?

> Прекинете ја интернет врската, не внесувајте лозинки, и веднаш пријавете на ИТ Секторот. Брзата реакција ја ограничува штетата.

Речник и чек-листа

Поим	Значење
Malware	Малициозен софтвер — општ поим за штетни програми
Ransomware	Софтвер што заклучува податоци и бара откуп
Тројанец	Малициозен програм маскиран како легитимен
Социјален инженеринг	Манипулација на луѓе за откривање информации
VPN	Виртуелна приватна мрежа за безбедна врска
Двофакторна автентикација	Втор слој заштита при најава
Резервна копија	Копија на податоци за враќање при загуба

Основна сајбер хигиена

- ✓ Силни и уникатни лозинки + 2FA
- ✓ Ажурирани системи и антивирус
- ✓ Внимание со е-пошта, линкови и прилози
- ✓ VPN на јавни мрежи
- ✓ Редовни резервни копии
- ✓ Пријавување на секое сомнение

Сајбер безбедност и надвор од работа

Добрите навики за сајбер безбедност не завршуваат кога ќе го напуштите работното место. Заштитата на вашиот дигитален живот дома е подеднакво важна — и често истите принципи ве штитат и на работа и приватно.

Домашна мрежа

- ✓ Сменете ја стандардната лозинка на домашниот рутер
- ✓ Користете силна лозинка за домашниот WiFi
- ✓ Ажурирајте го рутерот кога има достапни надградби
- ✓ Одвојте гостинска мрежа за посетители

Заштита на семејството

- ✓ Разговарајте со семејството за сајбер ризиците
- ✓ Помогнете им да препознаваат измами
- ✓ Внимавајте на безбедноста на децата на интернет
- ✓ Одржувајте ги домашните уреди ажурирани и заштитени

Заедничка култура. Сајбер безбедноста е начин на размислување, не сет од правила само за работа. Кога станува навика во секој аспект од животот, вие и вашите блиски сте многу побезбедни.

Континуирано учење

Технологијата и заканите постојано се менуваат. Останете информирани, следете ги препораките и не двоумете се да прашате кога сте во дилема. Учењето за сајбер безбедност е патување што трае цел живот.

Заклучок

Сајбер безбедноста е континуиран процес, не еднократна активност. Заканите ќе се менуваат, но основните принципи остануваат: бидете внимателни, скептични кон неочекуваното, и одржувајте добри дигитални навики.

> **Клучна порака.** Вие сте најважната линија на одбрана. Секоја информирана одлука што ја носите ја зголемува безбедноста на вас и на целата организација.