МЕПСО

ПРИРАЧНИК

Прирачник за безбедност на е-пошта

Заштита од phishing, малициозни прилози и измами преку електронска пошта

Придружен материјал за обуката:
„Безбедност на е-пошта"

Документ бр. МЕПСО-ПРИ-МАИЛ-002 · Класификација: Интерна употреба
Сектор за информатичка и сајбер безбедност · МЕПСО АД Скопје

Содржина

1. Вовед

Електронската пошта е најкористениот деловен алат за комуникација — и токму затоа најчестата влезна точка за сајбер напади. Над 90% од успешните напади започнуваат со е-пошта.

Овој прирачник ќе ви помогне да ги препознаете заканите што пристигнуваат преку е-пошта и да развиете навики што ве штитат вас и организацијата. Нема да ве направи технички експерт — ќе ве направи внимателен и информиран корисник, што е поважно.

Секој ден добивате десетици пораки. Меѓу нив, повремено се крие некоја што е дизајнирана да ве измами, да украде податоци или да инсталира малициозен софтвер. Разликата помеѓу безбеден и компромитиран систем често е еден клик.

Клучна мисла. Најсофистицираните безбедносни системи можат да бидат заобиколени со една добро осмислена е-пошта која ќе измами човек да кликне. Вие сте најважната заштита.

2. Зошто е-поштата е мета на напади

Напаѓачите ја сакаат е-поштата од неколку причини:

- **Досег** — една порака може да се испрати до илјадници луѓе истовремено;
- **Доверба** — луѓето навикнале да отвораат пораки и да кликаат линкови;
- **Лесна имитација** — релативно лесно е да се преправиш дека си некој друг;
- **Директен пристап** — е-поштата води директно до корисникот, заобиколувајќи многу технички заштити;
- **Човечки фактор** — искористување на љубопитност, страв или итност.

2.1 Што сакаат да постигнат

Цел	Метод
Кражба на лозинки	Лажни страници за најава
Инсталирање малициозен софтвер	Заразени прилози
Финансиска измама	Лажни фактури, барања за трансфер
Кражба на податоци	Манипулација да откриете информации
Пристап до системи	Компромитирање на корисничка сметка

3. Анатомија на е-пошта закана

За да препознаете сомнителна порака, важно е да ги знаете деловите што напаѓачите ги искористуваат.

3.1 Адреса на испраќачот

Најважниот елемент за проверка. Напаѓачите користат адреси што личат на легитимни, со мали разлики што лесно се пропуштаат — заменета буква, дополнителен знак, сличен домен.

> **Внимавајте.** Адреса како mepso-it.com не е исто што и mepso.com.mk. Секогаш проверувајте го целиот домен, не само името што се прикажува.

3.2 Наслов (Subject)

Насловите се дизајнирани да предизвикаат итна реакција: „Итно", „Вашата сметка е блокирана", „Последно предупредување". Итноста е тактика за да не размислувате трезвено.

3.3 Тело на пораката

Обрнете внимание на генерички поздрави („Почитуван корисник" наместо вашето име), граматички грешки, необичен тон, и барања да направите нешто брзо.

3.4 Линкови и прилози

Тука се крие вистинската опасност. Линковите водат до лажни страници, а прилозите содржат малициозен код.

4. Phishing — препознавање и заштита

Phishing е најчестиот тип на напад преку е-пошта. Напаѓачот се преправа дека е доверлива институција за да ве наведе да откриете чувствителни податоци.

4.1 Видови phishing

Вид	Опис
Масовен phishing	Иста порака до илјадници примачи
Spear phishing	Насочен кон конкретна личност со лични детали
Whaling	Насочен кон раководители и високи функции
Clone phishing	Копија на легитимна порака со изменети линкови

4.2 Црвени знамиња

- ✓ Итност и притисок за брза акција
- ✓ Барање за лозинка, ПИН или лични податоци
- ✓ Генерички поздрав наместо вашето име
- ✓ Граматички и правописни грешки
- ✓ Сомнителна адреса на испраќачот
- ✓ Премногу добра понуда (награди, добивки)
- ✓ Линкови што не се совпаѓаат со прикажаниот текст

> **Пример на phishing:**
> „Почитуван корисник, забележавме невообичаена активност на вашата сметка. За да ја потврдите, кликнете овде и внесете ги вашите податоци во рок од 2 часа, инаку сметката ќе биде трајно блокирана."
>
> *Знаци:* генеричен поздрав, итност, барање податоци, притисок.

4.3 Како да се заштитите

- ✓ Застанете пред да реагирате на итни барања
- ✓ Проверете ја адресата на испраќачот внимателно
- ✓ Поминете со глувчето врз линкот за да ја видите вистинската адреса
- ✓ Рачно внесувајте адреси во прелистувачот наместо преку линкови
- ✓ Никогаш не внесувајте лозинка на страница до која сте стигнале преку линк
- ✓ При сомнеж, потврдете преку официјален телефон

5. Малициозни прилози

Прилозите се чест начин за ширење на малициозен софтвер. Отворањето на заразен прилог може да инсталира вирус, ransomware или шпионски програм.

5.1 Опасни типови на датотеки

Тип	Ризик
.exe, .scr, .bat	Извршни програми — висок ризик
.zip, .rar	Компресирани датотеки што кријат содржина
.docm, .xlsm	Документи со макроа што извршуваат код
.js, .vbs	Скрипти што извршуваат команди

Правило. Не отворајте прилози од непознати испраќачи. Дури и од познати, ако не сте ја очекувале датотеката, потврдете преку друг канал пред да отворите.

5.2 Макроа во документи

Кога отворате документ што бара „Овозможи макроа" — застанете. Легитимните документи ретко го бараат ова. Овозможувањето макроа може да изврши малициозен код.

6. Опасни линкови

Линковите се маскираат за да изгледаат безбедни, но водат до опасни страници.

6.1 Како да проверите линк

- ✓ Поминете со глувчето врз линкот (без клик) — вистинската адреса се појавува долу
- ✓ Проверете дали доменот се совпаѓа со очекуваниот
- ✓ Внимавајте на скратени линкови што ја кријат вистинската дестинација
- ✓ Ако линкот бара да внесете податоци, бидете особено претпазливи

Совет. Ако добиете порака од банка или институција со линк, не кликајте. Наместо тоа, отворете нов прозорец и рачно внесете ја официјалната адреса. Така сте сигурни дека сте на вистинската страница.

7. Спам и нежелена пошта

Спамот е нежелена масовна пошта. Иако често е само досаден, може да содржи и закани.

- ✓ Не одговарајте на спам — тоа потврдува дека адресата е активна
- ✓ Не кликајте „отпиши се" во сомнителни пораки — може да биде замка
- ✓ Означувајте спам за да го подобрите филтрирањето
- ✓ Не ја објавувајте вашата деловна адреса на јавни места непотребно

8. Компромитирана деловна е-пошта (BEC)

Business Email Compromise е софистициран напад каде напаѓачот се преправа дека е

раководител или партнер за да наведе финансиска трансакција или откривање податоци.

8.1 Типичен сценарио

Добивате порака што изгледа дека е од директор, со итно барање за трансфер на средства или испраќање доверливи податоци. Тонот е авторитативен и итен.

> **Внимание.** Секое необично барање за трансфер на пари или доверливи податоци, дури и ако изгледа дека е од раководител, треба да се потврди преку директен телефонски повик или лична комуникација.

8.2 Заштита

- ✓ Потврдувајте необични финансиски барања преку втор канал
- ✓ Внимавајте на промени во деталите за плаќање
- ✓ Не се потпирајте само на е-пошта за важни трансакции
- ✓ Пријавете сомнителни барања веднаш

9. Шифрирање и приватност

Чувствителните информации испратени преку е-пошта треба да бидат заштитени.

- ✓ Не испраќајте лозинки или доверливи податоци во обичен текст
- ✓ Користете шифрирање за чувствителни прилози каде е достапно
- ✓ Внимавајте на кого испраќате — двојно проверете ги примачите
- ✓ Избегнувајте „Одговори на сите" освен ако е навистина потребно

> **Чест грешка.** Случајно испраќање на доверлива информација на погрешен примач е чест инцидент. Секогаш проверете ја адресата на примачот пред да притиснете „Испрати", особено кога автоматското комплетирање предлага адреса.

10. Добри навики при секојдневна употреба

- ✓ Прегледувајте ги пораките внимателно пред да реагирате
- ✓ Проверувајте ги адресите на испраќачите
- ✓ Не кликајте на линкови или прилози при најмал сомнеж
- ✓ Користете силна и уникатна лозинка за е-поштата
- ✓ Вклучете двофакторна автентикација
- ✓ Одјавувајте се од е-поштата на споделени уреди
- ✓ Пријавувајте сомнителни пораки

11. Што да правите при инцидент

Ако сте кликнале на сомнителен линк, отвориле прилог или внеле податоци некаде каде не требало:

1. Не паничете — брзата реакција е клучна
2. Прекинете ја врската со интернет ако се сомневате на малициозен софтвер
3. Веднаш променете ги лозинките што сте ги внеле

4. Пријавете на Секторот за информатичка безбедност
5. Не бришете ја пораката — може да послужи за анализа

> **Не се срамете да пријавите.** Секој може да направи грешка. Брзото пријавување овозможува тимот за безбедност да реагира и да ја ограничи штетата. Тишината само го влошува проблемот.

Практични сценарија

Сценарио 1: Итна порака од „директорот"

Добивате е-пошта наводно од генералниот директор, со итно барање да платите фактура на нова сметка, „бидејќи е во состанок и не може да се јави".

> **Правилна реакција:** Не постапувате веднаш. Потврдувате директно со директорот или преку официјален канал. Итноста и невозможноста да се провери се класични знаци на BEC измама.

Сценарио 2: Проследена фактура

Колега ви проследува фактура за плаќање со прилог. Прилогот бара да овозможите макроа за да го видите содржината.

> **Правилна реакција:** Не овозможувате макроа. Проверувате со колегата дали навистина ја испратил и дали очекувал макроа. Легитимните фактури не бараат макроа.

Сценарио 3: Известување за пакет

Добивате порака дека имате недоставен пакет и треба да кликнете линк за да ја платите испораката.

> **Правилна реакција:** Не кликате. Ако очекувате пакет, одите директно на официјалната страница на курирската служба. Лажните известувања за пакети се многу чести.

Најчесто поставувани прашања

Како да знам дали адресата на испраќачот е лажна?

> Проверете го целиот домен внимателно, не само прикажаното име. Барајте мали разлики — заменети букви, дополнителни знаци, сличен но не идентичен домен.

Дали е безбедно да отворам PDF прилог?

> PDF-ите генерално се побезбедни од извршни датотеки, но и тие можат да содржат малициозен код. Отворајте ги само од доверливи испраќачи што сте ги очекувале.

Што ако кликнав линк но не внесов ништо?

> Сепак пријавете. Некои линкови можат да инсталираат малициозен софтвер само со отворање. Тимот за безбедност ќе процени дали има ризик.

Дали филтерот за спам ме штити целосно?

> Не. Филтрите фаќаат многу, но не сè. Најсофистицираните напади често поминуваат. Вашата внимателност останува неопходна.

Може ли да ми се украде лозинката само со отворање порака?

> Ретко, но можно е со некои напредни напади. Затоа не отворајте пораки од непознати испраќачи, и никогаш не внесувајте податоци преку линк од порака.

Речник и чек-листа

Поим	Значење
Phishing	Измама преку лажни пораки за кражба на податоци
Spear phishing	Насочен phishing кон конкретна личност
BEC	Компромитирана деловна е-пошта — измама преку лажен идентитет
Малициозен прилог	Датотека што содржи штетен код
Макро	Автоматизирана команда во документ, може да биде злоупотребена
Спам	Нежелена масовна пошта
Домен	Делот од адресата по знакот @

Брза чек-листа пред секој клик

- ✓ Дали ја познавам и очекувам адресата на испраќачот?
- ✓ Дали насловот создава вештачка итност?
- ✓ Дали пораката бара лозинка или лични податоци?
- ✓ Каде навистина води линкот (проверено со глувчето)?
- ✓ Дали очекував овој прилог?
- ✓ При сомнеж — дали пријавив наместо да кликнам?

Улога на е-поштата во работењето на МЕПСО

Како оператор на критична инфраструктура, МЕПСО има зголемена одговорност за заштита на комуникацијата. Е-поштата често содржи чувствителни оперативни и деловни информации чие компромитирање може да има последици надвор од самата организација.

Дополнителни мерки за критична инфраструктура

- ✓ Оперативните податоци никогаш не се испраќаат преку незаштитени канали
- ✓ Комуникацијата со надворешни партнери подлежи на дополнителна проверка
- ✓ Пристапот до деловната е-пошта од лични уреди се контролира
- ✓ Редовно се спроведуваат симулации на phishing за подигање на свеста

> **Заедничка одговорност.** Безбедноста на е-поштата не е само задача на ИТ Секторот. Секој вработен што ракува со е-пошта е дел од одбранбениот систем на организацијата. Вашите навики директно влијаат на безбедноста на целата инфраструктура.

Периодична обука

Заканите постојано се менуваат и стануваат посложени. Затоа е важно редовно да ги освежувате знаењата преку обуки и да останете информирани за новите методи на измама. Овој прирачник е дел од таа континуирана едукација.

Заклучок

Е-поштата ќе остане централен дел од работата — и централна мета на напади. Вашата внимателност е најдобрата заштита. Секоја порака што внимателно ја проверувате, секој сомнителен линк што не го кликате, секое пријавување — сето тоа ја гради безбедноста на МЕПСО.

> **Запомнете.** Кога сте во дилема, застанете и прашајте. Една минута претпазливост може да спречи голем инцидент.

МЕПСО АД Скопје — Оператор на електропреносниот систем на Северна Македонија
Документ бр. МЕПСО-ПРИ-МАИЛ-002 · Класификација: Интерна употреба