# Безбедност на Интернет

Можностите на интернет се практично бескрајни. Интернетот овозможува брз пристап до информации, глобална комуникација и разни други функции. Сепак, тој содржи и опасности како малициозен софтвер, спам и фишинг. За да ја осигурате вашата безбедност на интернет, од клучно значење е да бидете свесни за овие закани и да знаете како да се оддалечите од нив.

## Креирање силни лозинки

Ќе треба да **креирате лозинка** за да правите речиси сè на Интернет, од проверка на вашата е-пошта до онлајн банкарство. И иако е поедноставно да се користи кратка лозинка која лесно се памети, тоа може да претставува и **сериозни ризици** за вашата онлајн безбедност. За да се заштитите себе си и вашите информации, ќе сакате да користите лозинки што се **долги** , **силни** и **тешки за некој друг да ги погоди** , додека сеуште ги чувате релативно **лесно за запомнување** .

Иако повеќето веб-локации се безбедни, секогаш постои мала шанса некој да се обиде да пристапи или да ги украде вашите информации. Ова е попознато како **хакирање** . Силната лозинка е еден од најдобрите начини за одбрана на вашите сметки и приватни информации од хакери.

Насоки за изработка на безбедни лозинки Изработката на безбедна лозинка вклучува создавање на нешто незаборавно за вас, но предизвик за другите да го погодат. Еве основни совети што треба да ги имате на ум:

- Избегнувајте да внесувате лични податоци како вашето име, роденден, корисничко име или е-пошта во вашата лозинка, бидејќи тие често може лесно да се најдат и погодат.
- Инсистирајте на подолги лозинки. Стремете се кон минимум шест знаци, иако повеќе знаци значат зголемена безбедност.

- Користете единствени лозинки за различни сметки за да спречите една компромитирана лозинка да ги загрози сите ваши сметки.
- Вклучете мешавина од броеви, симболи и големи и мали букви.
- Ослободете се од зборови од речник, бидејќи тие лесно може да се скршат. На пример, „школо1“ е слаб избор.
- Најбезбедните лозинки се случајни. Ако создавањето е предизвик, размислете да користите генератор на лозинки за помош.

Некои од најчесто користените лозинки се засноваат на **семејни имиња**, **хоби** или само **едноставна шема**. Иако овие типови лозинки се лесни за запомнување, тие се и некои од најмалку безбедните.

## Безбедносните карактеристики на вашиот прелистувач

Кога сурфате на Интернет, вашиот компјутер е изложен на разни закани како вируси, малициозен софтвер и шпионски софтвер. За среќа, вашиот веб-прелистувач е опремен со бројни безбедносни карактеристики за да го заштити вашиот систем. Ќе истражиме некои од клучните карактеристики за кои треба да знаете, заедно со лесни за следење совети за подобрување на вашата безбедност на интернет.

### Проверете ја веб-адресата

Злонамерните веб-локации често користат погрешни веб-адреси за да ги измамат корисниците. Земете, на пример, веб-локација како **www.bankofarnerica.com** , која многу наликува на **www.bankofamerica.com** , но суптилно го заменува 'm' со ' rn '.

За да потврдите дека посетувате легитимна, доверлива локација, а не лажна со слична адреса, важно е внимателно да го проверите името на доменот. Многу веб-прелистувачи помагаат во ова со истакнување на името на доменот во потемна боја во лентата за адреси за да биде позабележително. На пример, во лентата за адреси, оригиналниот bankofamerica.com ќе биде нагласен за да помогне да се разликува од сајтовите со измами.

## Погледнете го безбедносниот симбол

Некои веб-локации ќе прикажат **симбол за заклучување** во лентата за адреси. Ова најчесто се гледа кај одредени типови на веб-локации, како што се онлајн продавници и банкарски сајтови. Ова значи дека веб-локацијата користи **HTTPS** врска, што го прави безбедно да ги внесете вашите лични податоци. Ќе видите и **https** на почетокот на URL-то.


Нема да го гледате овој симбол на сите веб-локации и тоа е во ред - на сите веб-локации не им е потребен овој дополнителен слој на безбедност. Сепак, треба да избегнувате да внесувате какви било чувствителни информации, како што е бројот на вашата кредитна картичка, ако не го гледате овој симбол во лентата за адреси.

# Избегнување на спам и фишинг

Интернетот, кој опфаќа е-пошта, инстант пораки и социјални медиуми, е витална алатка за комуникација. Сепак, тоа е исто така вообичаено игралиште за измамници и сајбер-криминалци. За да се заштитите од измами со е-пошта, штетен софтвер и кражба на идентитет, од клучно значење е да научите како да забележите и да се оттргнете од потенцијално штетната содржина во вашето сандаче, како што се спам и напори за фишинг.

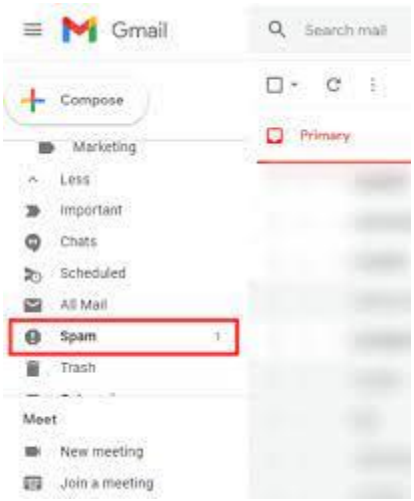
**Справување со спам**

Спам, исто така познат како несакана е-пошта, го пополнува вашето сандаче со несакани реклами и може да ги скрие ризиците како фишинг

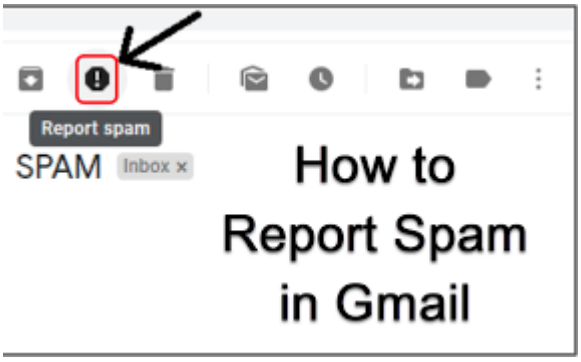
и малициозен софтвер. Повеќето услуги за е-пошта нудат функции кои помагаат да се филтрира спам, со што вашето сандаче е побезбедно.

**Филтри за спам**

Филтрите за спам ги сортираат потенцијалните спам во папка за спам за да спречат случајно отворање. Сепак, овие системи не се сигурни, а и оригиналните е-пошта може да се филтрираат. Препорачливо е редовно да ја проверувате вашата папка со спам за пропуштени важни пораки:




Многу услуги за е-пошта исто така имаат функција што можете да ја користите за означување на е-пошта како спам. Во Gmail, на пример, можете да ја изберете пораката и да кликнете на копчето **Обележи како спам**. Ова му помага на вашиот давател на е-пошта да ги филтрира овие типови пораки во иднина:



## Фишинг

Фишинг-измамите се измамнички пораки насочени кон добивање на вашите чувствителни информации, како лозинки или броеви на кредитни картички, често претставувајќи се како банки или доверливи ентитети. Иако може да изгледаат автентични, измамниците лесно создаваат убедливи детали. Еве како измама го користи името на DHL за фишинг:


## Други вообичаени измами со е-пошта

Спам и фишинг се распространети, но постојат и други измами со е-пошта. Некои нудат големи суми пари во замена за однапред исплата, додека други имитираат контакти што ги познавате, бараат пари или ве поттикнуваат да преземете прилози.

Бидете внимателни како со спам и фишинг. Избегнувајте испраќање пари врз основа на барање за е-пошта и внимавајте на неочекувани прикачувања, бидејќи тие можат да содржат малициозен софтвер кој го загрозува вашиот компјутер и лични податоци.

Како што се развиваат тактиките за спам, измами и фишинг, информираноста за тоа што да внимавате и да избегнувате помага да се заштитат вашето сандаче и компјутер.

## Безбедно онлајн купување

**Онлајн купувањето** е пригоден начин да купите речиси сè од удобноста на вашиот дом. И додека има некои ризици со купувањето преку Интернет, постојат и многу начини да се заштитите себеси и вашите финансиски информации. Некои совети како што следува:

1. Купување од дома - за подобра заштита на чувствителните детали како што се броевите на кредитните картички, препорачливо е да купувате користејќи ја домашната интернет конекција. Купувањето на јавен Wi-Fi или користењето јавни компјутери, како оние во библиотеките, го зголемува ризикот од хакирање и потенцијално ги загрозува вашите информации.
2. Безбедност на HTTPS - Побарајте симбол за заклучување во лентата за адреси на веб-локацијата, обично видлив на страницата за плаќање на онлајн продавницата. Ова укажува на HTTPS конекција, обезбедувајќи ги податоците што ги внесувате. Иако сите страници на шопинг сајтот нема да го имаат овој симбол, избегнувајте да внесувате финансиски информации на страниците без него.
3. Истражување пред купување - од суштинско значење е да се истражува онлајн компанија или продавач пред да се купи. Потврдете ја нивната физичка адреса и бројот за контакт за какви било проблеми. Проверете ги прегледите на клиентите на платформи како Yelp и Google за да ја процените нивната репутација.
4. Безбедни начини на плаќање - Кредитните картички често се најбезбедниот начин на плаќање преку Интернет. Најдобро е да избегнувате директни жични трансфери, банкарски трансфери или испраќање готовина/чекови. За дополнителна безбедност, размислете за користење онлајн услуги за плаќање како PayPal или Google Wallet.

5. Водете евиденција за трансакции - Водете евиденција за онлајн трансакции, вклучувајќи сметки, броеви на нарачки, детали за производот и цени. Исто така, чувајте ги е-поштата од продавачите, бидејќи тие можат да бидат корисни во случај на спорови или проблеми.

## Безбедност на Интернет за деца

За да ја осигурате безбедноста на вашите деца на интернет, важно е да бидете свесни за различните интернет ризици. Може да наидат на несоодветна содржина, како порнографија или експлицитен јазик. Дополнително, постои ризик од сајбер малтретирање или онлајн малтретирање. Иако не е сигурно дека вашето дете ќе се соочи со сите овие закани, информираноста за нив може да ве води вас и вашите деца да правите побезбедни избори на интернет. Еве неколку клучни упатства за едукација на вашите деца да останат безбедни на интернет:

1. Едуцирајте се за Интернет: Разбирањето на Интернет ви помага да ги разберете ризиците и ефективно да комуницирате со вашите деца за нив.
2. Воспоставете онлајн правила: Поставете јасни граници за тоа што вашите деца можат и што не можат да прават онлајн. Креирањето насоки пред да се појават какви било проблеми е од клучно значење.
3. Безбедност на личните информации: поучете ги вашите деца за опасностите од споделување лични податоци како телефонски броеви, адреси и информации за кредитна картичка. Таквите податоци може да бидат злоупотребени од криминалци за да му наштетат на вашето семејство.
4. Безбедно социјално вмрежување: Научете ги вашите деца одговорно да ги користат социјалните медиуми. Потсетете ги дека сè што е споделено на интернет, дури и со пријателите, може да заврши во погрешни раце. Тие треба да објавуваат само она што им е пријатно да го гледа целиот свет.
5. Отворена комуникација: Охрабрете ги вашите деца да ви пристапат со какви било прашања на интернет. Важно е да се

разбере дека случајно можат да налетаат на несоодветна содржина, дури и со најдобри намери.

6. Редовни Интернет дискусии: Водете постојани разговори со вашите деца за нивната употреба на интернет. Честите дискусии може да ги направат поудобно да ви пристапат со какви било проблеми со кои би можеле да се сретнат.

**Честитки, научивте како безбедно да користите Интернет!**