MKSafeNet

Безбеден интернет

паметно и безбедно користење на интернетот

Зошто е важна интернет безбедноста?

Интернет-безбедноста е клучна за заштита на нашите лични податоци, приватност и дигитален идентитет од злоупотреби и сајбер-напади.

Таа ни овозможува сигурно и одговорно користење на интернетот во секојдневниот живот.

MKSafeNet

Број на сајбер-напади во изминатите години

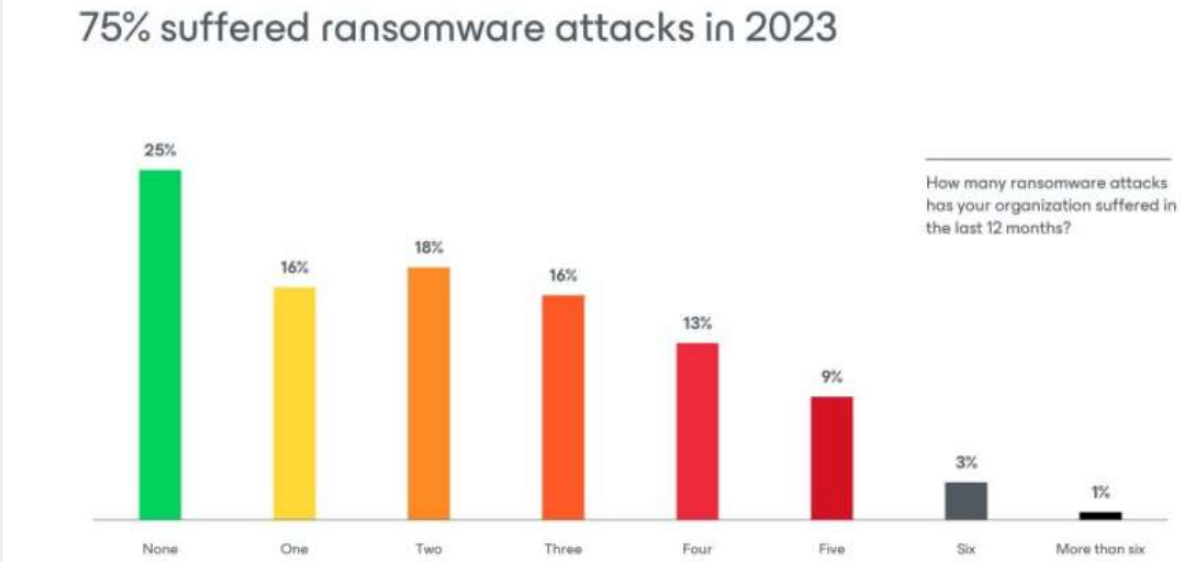
MKSafeNet

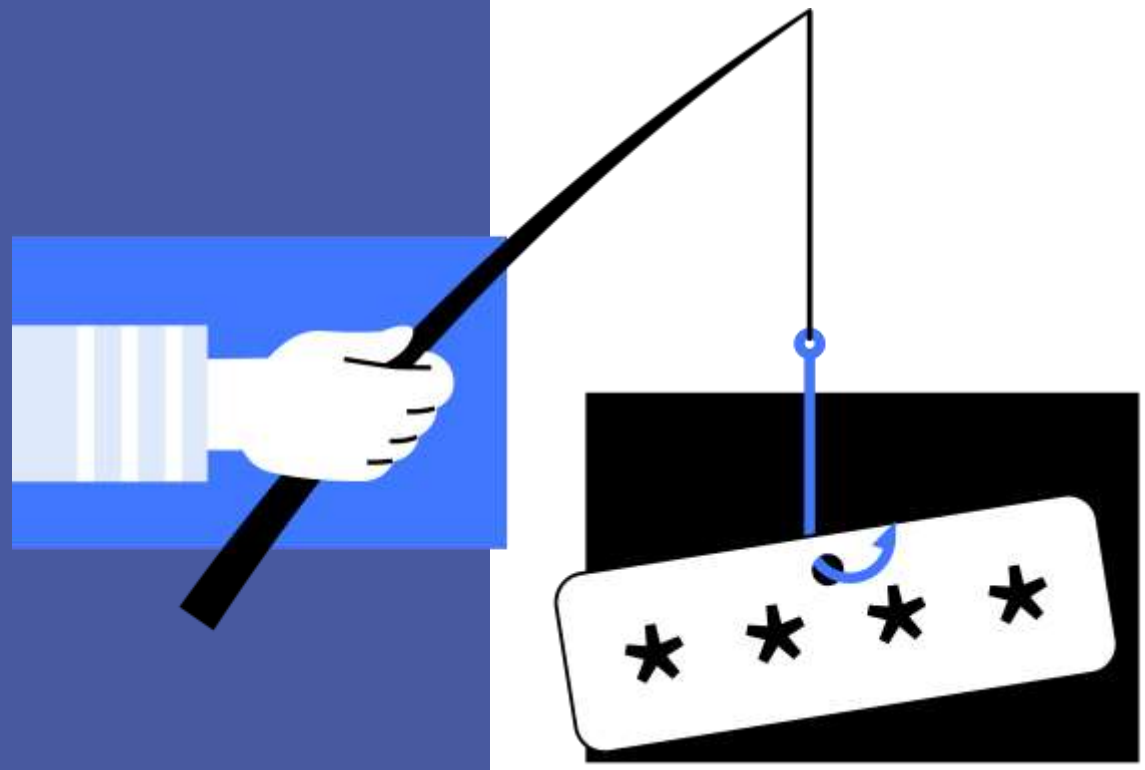
Потенцијални закани на интернет

Малициозен софтвер (Malware)

Малициозниот софтвер, како што се вируси, тројанци и ransomware, може да ги зарази уредите и да ги оштети или заклучи вашите податоци, барајќи откуп за нивно враќање. Често се крие во сомнителни линкови, прилози во е-пошта или нелегални програми, и може да предизвика сериозни финансиски и технички проблеми. Особено е опасно кога се шират преку лажни апликации или веб-страници кои се преправаат дека се легитимни, па затоа е важно секогаш да ја проверувате автентичноста на изворите пред да кликнете или преземате нешто.

75% од организациите претрпеле барем еден ransomware напад



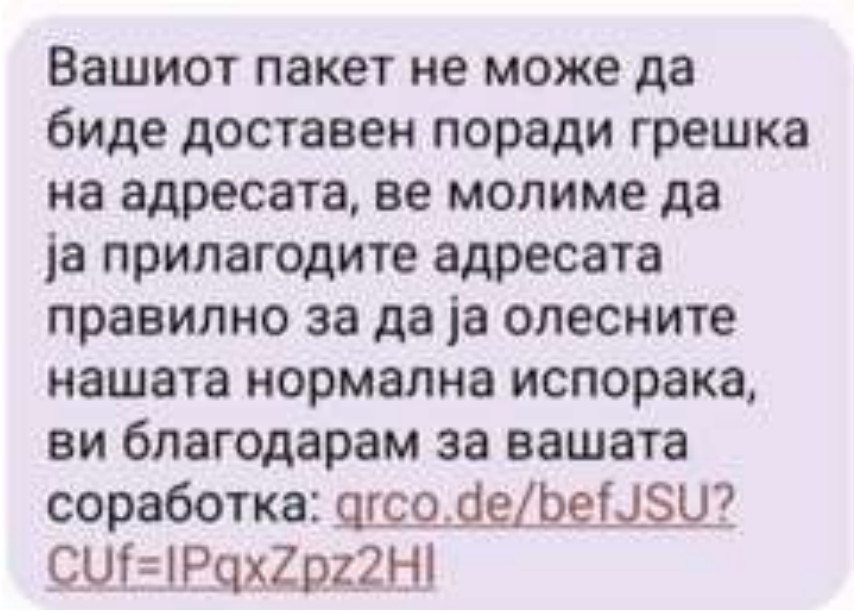


Фишинг напади

Фишинг нападите се најчестиот облик на онлајн измами, при што напаѓачите создаваат лажни веб-страници или пораки кои изгледаат автентично.

Главната цел е да ги натераат жртвите да внесат лични податоци, како кориснички имиња, лозинки или банкарски детали, што потоа може да се злоупотребат.

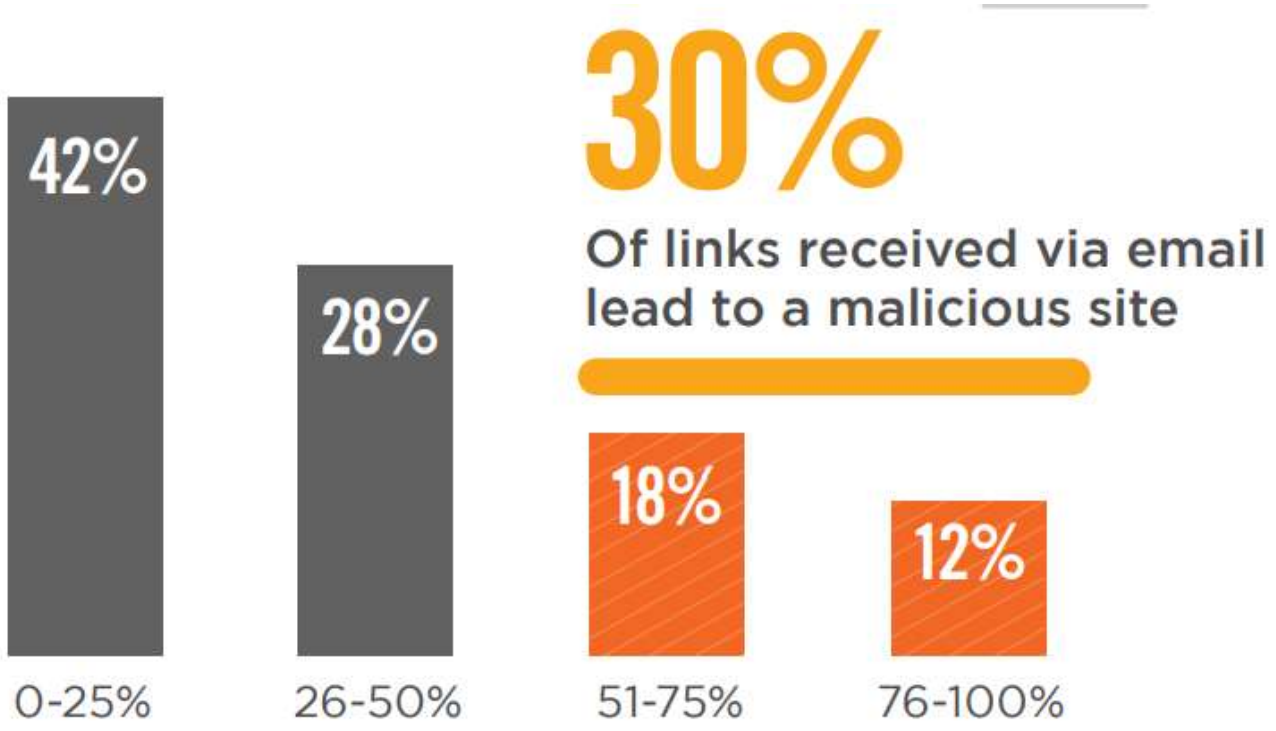
Како да препознаете фишинг напад



Проверете ги URL-адресите за необични домени или правописни грешки, бидејќи напаѓачите често користат лажни адреси кои личат на официјални.

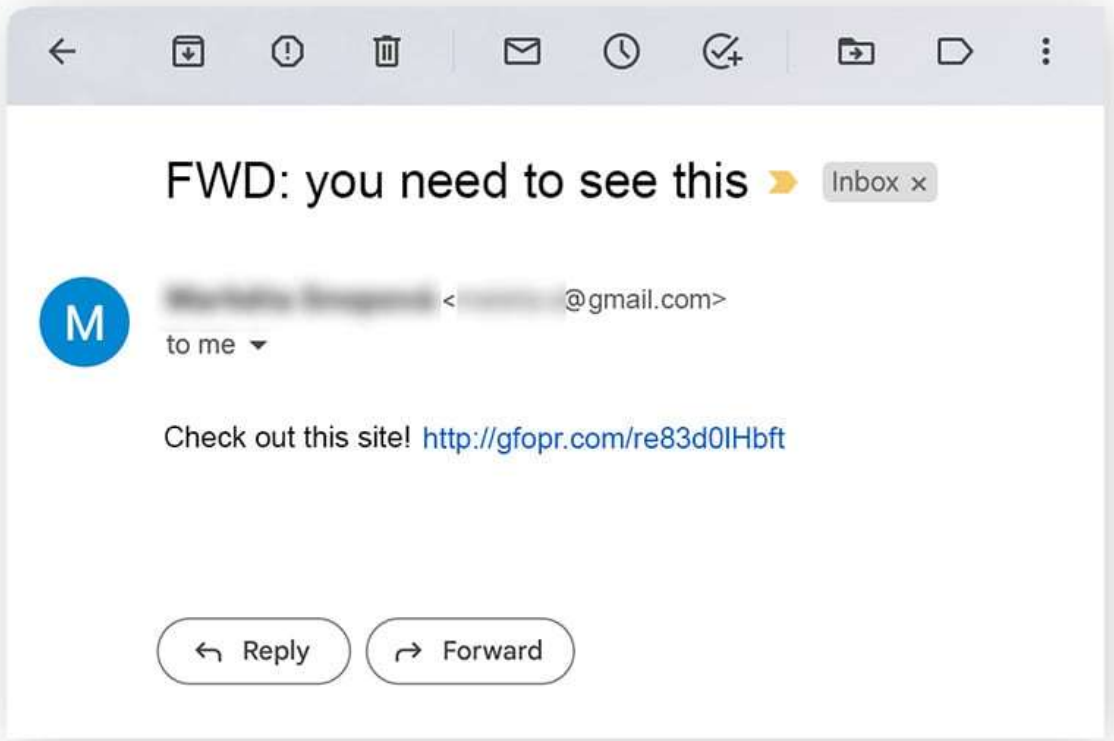
Ако сомневате, секогаш контактирајте ја компанијата или лицето директно преку официјален канал за да ја потврдите автентичноста на пораката.

Опасност од малициозни линкови



Социјален инженеринг

Напаѓачите кои користат социјален инженеринг, често се претставуваат како пријатели, колеги или авторитетни лица за да ја добијат вашата доверба. Со оваа техника, тие можат да манипулираат и да ве убедат да споделите доверливи информации или да направите несигурни активности. За да се заштитите, бидете скептични кон неочекувани барања за информации, дури и ако доаѓаат од познати лица, и секогаш потврдете ја идентитетот на лицето преку друг канал на комуникација.



Не споделувајте чувствителни податоци, како лозинки или финансиски информации, без да осигурате дека комуникацијата е сигурна и автентична.

Злоупотреба на приватноста

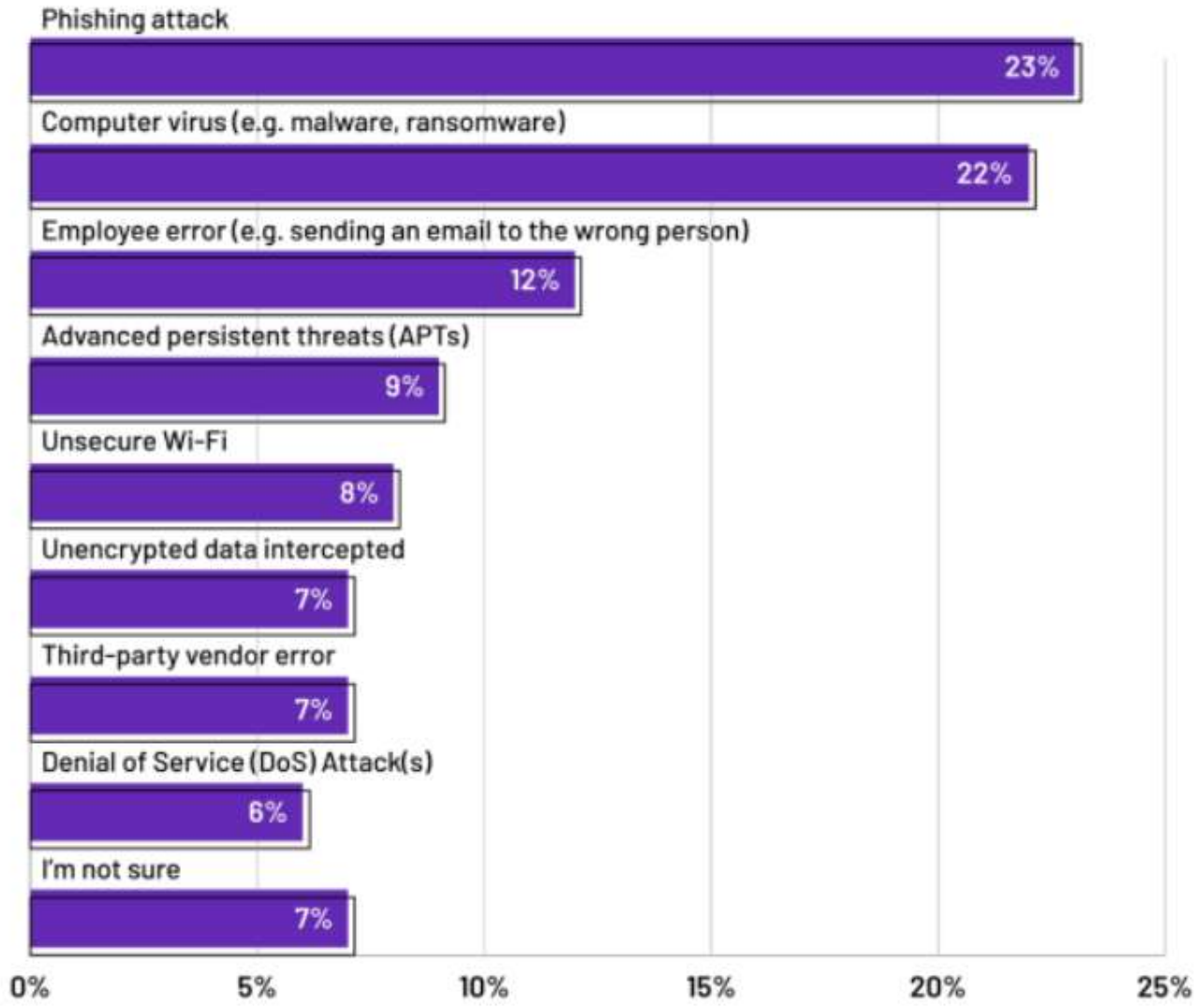
Вашите податоци, како локација, навики на пребарување и фотографии, можат да се соберат и продадат без ваше знаење. Оваа практика, покрај тоа што е нарушување на вашата приватност, може да се искористи за таргетирани реклами, финансиски измами или идентитетска кражба.

Кражба на идентитет

Криминалците можат да ги искористат вашите лични информации за да отвораат кредитни сметки, да прават онлајн трансакции или да се претставуваат како вас во комуникација. Ова може да има долгорочни последици врз вашата финансиска стабилност и репутација. За да се заштитите проверувајте банкарски изводи за сомнителни активности, користете силни лозинки, активирајте двостепена автентикаија, при сомнеж за кражба за идентите веднаш контактирајте ја банката и властите.

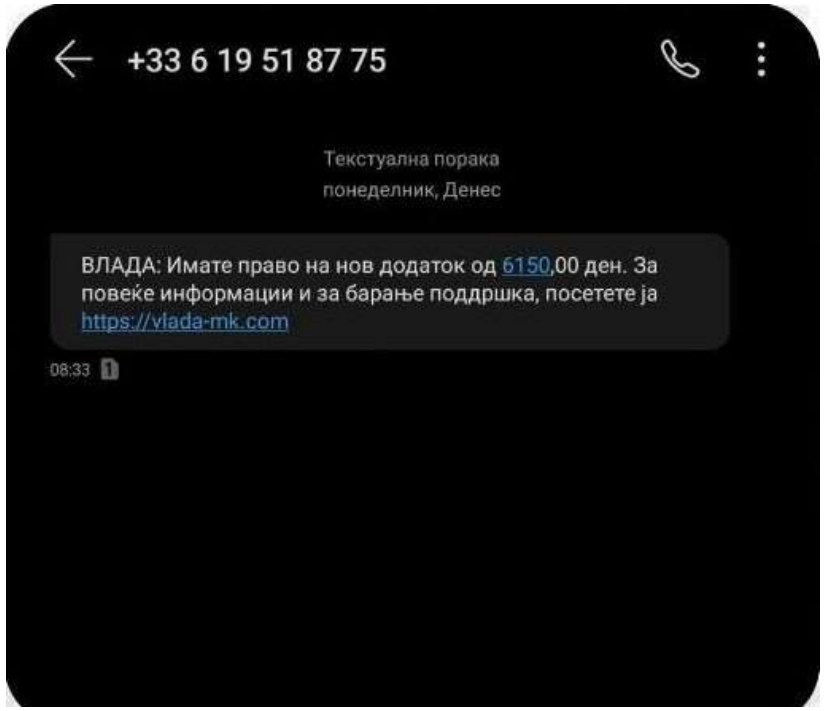
MKSafeNet

Најчести видови на сајбер-напади



Онлајн измами

Лажните понуди и награди, пирамидалните шеми или сомнителните веб-страници за е-трговија често ветуваат премногу за да бидат вистинити. Ваквите измами можат да резултираат со директни финансиски загуби или кражба на податоци.




Почетна / Вести / Падна уште една „пирамида" во Македонија: DGPT како CONTI

ВЕСТИ

Падна уште една „пирамида" во Македонија: DGPT како CONTI

By kotlina • 20.10.2024

MKSafeNet

Заштита од закани

Како да реагирате во случај на сајбер напад

Доколку станете жртва на сајбер напад, најважно е веднаш да реагирате за да го минимизирате оштетувањето. Прво, променете ги сите компромитирани лозинки и известете ги релевантните служби, како ИТ поддршка или надлежни безбедносни органи. Доколку станува збор за финансиска измама, контактирајте ја вашата банка за да спречите дополнителни загуби. Исто така, анализирајте како се случил нападот за да преземете превентивни мерки и да избегнете слични инциденти во иднина.

Двостепена автентикација (2FA)

Двостепената автентикација додава дополнителен слој на сигурност со барање втор метод на потврда, како код испратен на вашиот телефон или биометриски податок. Ова значи дека дури и ако вашата лозинка биде компромитирана, напаѓачот нема да може да пристапи до вашата сметка без вториот чекор.
2FA е особено важно за е-пошта, банкарски услуги и социјални мрежи.

Користете силни лозинки

Силните лозинки се клучен елемент на онлајн безбедноста, бидејќи спречуваат неовластен пристап до вашите профили и чувствителни податоци. За да креирате безбедна лозинка, користете комбинација од големи и мали букви, броеви и специјални знаци, а истовремено избегнувајте лични информации како имиња и датуми на раѓање. Идеалната лозинка треба да биде долга најмалку 12 знаци и да биде уникатна за секоја платформа. Дополнително, користењето на менаџер за лозинки може да ви помогне да ги зачувате и управувате со сложените лозинки на безбеден начин.

Колку се безбедни вашите лозинки?

Дали знаевте дека лозинката **„password“** е една од најчесто користените и најлесно може да биде погодена?

- Хакерите можат да ја пробијат за помалку од една секунда!
- Други слаби лозинки се **„123456“**, **„qwerty“** и имиња без дополнителни знаци.
- **Колку е посилна вашата лозинка, толку е потешко да биде хакирана!**

Антивирусен софтвер

Антивирусниот софтвер помага да ги откриете и отстраните заканите, како што се вируси, шпионски софтвер и ransomware. **Редовно ажурирајте** го за да се осигурате дека препознава најнови видови на малициозен софтвер. Некои од најдобрите решенија на пазарот вклучуваат Norton, Bitdefender и Kaspersky. Бесплатни опции, како Windows Defender, исто така, нудат основна заштита.

Користете виртуелна приватна мрежа (VPN)

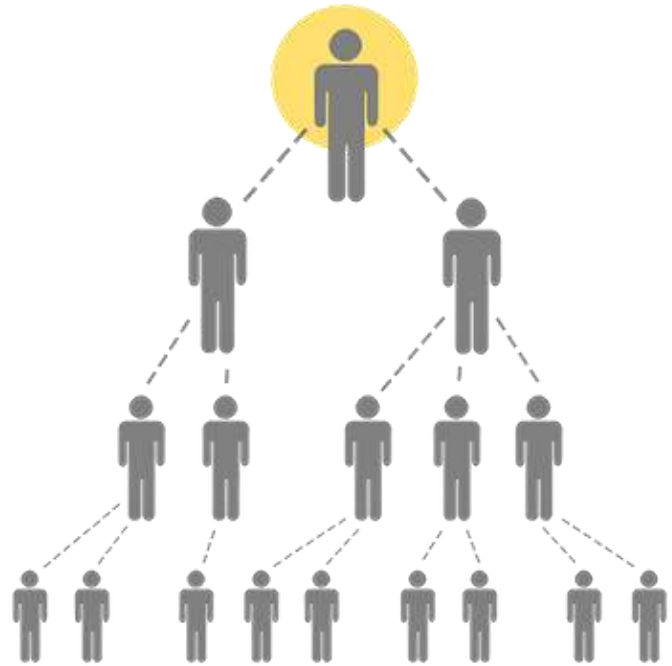
VPN (Virtual Private Network) е алатка која ја шифрира вашата интернет врска и ја крие вашата IP-адреса, обезбедувајќи поголема приватност и безбедност. Особено е корисна кога користите јавни Wi-Fi мрежи, бидејќи ги спречува хакерите да го пресретнат вашиот интернет сообраќај. Со VPN, вашите онлајн активности остануваат приватни, а пристапот до гео-ограничена содржина станува полесен. Сепак, важно е да изберете доверлив VPN сервис кој не ги продава вашите податоци.

Бидете внимателни со прилози и апликации

Кога преземате апликации, секогаш користете официјални платформи како **Google Play** или **App Store**, бидејќи тие имаат строги безбедносни проверки. Внимавајте на дозволите што ги бара апликацијата – ако некоја апликација бара пристап до податоци кои не се релевантни за нејзината функција, тоа е црвен флаг. Редовно бришете ги апликациите кои не ги користите и ажурирајте ги останатите за да осигурате дека имате најнови безбедносни поправки.

Како да препознаете пирамидална-шема?

1. **Големи ветувања** – Брзо и лесно збогатување без многу труд.
2. **Фокус на регрутирање** – Повеќе заработувате ако носите нови луѓе, а не од продажба на производи или услуги.
3. **Скапи вложувања** – Бараат од вас да платите висока сума однапред.
4. **Притисок за брзи одлуки** – „Зграпчете ја шансата пред да биде предоцна!“



Заштитете ја приватноста

За да ја заштитите вашата приватност, редовно проверувајте ги поставките за приватност на вашите социјални мрежи и апликации, ограничете ги дозволите за пристап до вашите податоци и користете алатки како VPN или прелистувачи фокусирани на приватност. Користете силни лозинки и избегнувајте да кликате на сомнителни линкови или да ги прифаќате сите колачиња (cookies) на веб-страниците. Исто така, бидете внимателни со она што го споделувате онлајн, бидејќи еднаш објавените информации може да бидат тешко да се повлечат.

Пазете се од јавен Wi-Fi

Јавните Wi-Fi мрежи, како оние во кафулиња или аеродроми, често се небезбедни и ранливи на напади. Хакерите можат да ги пресретнат вашите податоци, како лозинки и финансиски информации. За дополнителна заштита, користете виртуелна приватна мрежа (VPN), која го шифрира вашиот интернет сообраќај. Освен тоа, избегнувајте да вршите чувствителни активности, како онлајн банкарство, додека сте на јавни мрежи.

MKSafeNet

Онлајн однесување

Внимание на социјалните мрежи

Размислете пред да споделите на социјалните мрежи – информациите можат трајно да останат достапни и злоупотребени. Поставете приватност, ограничете пристап, и избегнувајте споделување чувствителни податоци како адреса или телефонски број. Користете ги поставките за приватност на платформите за да контролирате кој може да ги гледа вашите објави и податоци. Исто така, избегнувајте да споделувате информации за вашата локација во реално време, бидејќи тоа може да ги направи вас или вашиот дом ранлив на физички или дигитални закани.

Почитувајте ги правата на другите

Во онлајн просторот, почитувајте ги другите и воздржувајте се од омраза, навреди или ширење лажни информации. Социјалните мрежи се место за позитивен дијалог и конструктивна комуникација. Несоодветното однесување, како говор на омраза или клевета, може да доведе до правни последици или блокирање на вашите профили.Бидете свесни дека вашите зборови и активности онлајн можат да имаат долготрајни последици, не само за вас, туку и за другите. Поддржувајте инклузивна и почитувачка средина, каде што секој може да се изрази без страв од напади или дискриминација.

Дигитален отпечаток

Секогаш размислувајте за дигиталниот отпечаток што го оставате зад себе. Секоја објава, слика или коментар може да биде зачуван, а ова може да влијае на вашата иднина, било да се работи за вашата професионална репутација или лични односи. Обрнете внимание што и кога објавувате, и размислете дали ќе се чувствувате удобно ако истите податоци бидат достапни за јавноста.

MKSafeNet

Користење на онлајн платежни системи

Проверка на сигурноста на веб-страниците

1. Отворен катанец = небезбедна страница
2. Проверете за грешки во URL-адресата
3. “Претерано добри” попусти се сомнителни
4. Легитимни компании нема да бараат е-трансфери
5. Побарајте легитимна политика за приватност.
6. Осигурете се дека има валидна политика за враќање

Користење на виртуелни картички

Виртуелните картички, кои се генерираат за една трансакција, можат да обезбедат поголема сигурност при онлајн плаќање. Ова значи дека ако вашите податоци бидат украдени, тие нема да бидат поврзани со вашата главна картичка. Овој метод додава дополнителна заштита од измами при купување.

Проверка на трансакциите и сметките

Постојано следете ги своите трансакции и сметки за да откриете дали има неовластени плаќања или активности. Веќе многу банки и финансиски институции нудат алатки за автоматско известување за трансакции, кои ви овозможуваат брзо да реагирате ако нешто е сомнително.

Заклучок

- **Главни закани на интернет,** малициозен софтвер, фишинг напади и онлајн измами.
- **Практични совети за заштита**, како користење на двостепена автентикација, антивирусен софтвер и избегнување јавни Wi-Fi мрежи.
- **Онлајн однесување**, вклучувајќи почитување на правата на другите, одговорно користење на социјалните мрежи и следење на дигиталниот отпечаток.
- **Безбедно онлајн плаќање**, преку проверка на веб-страници, користење виртуелни картички и следење на трансакциите.

Со примена на овие знаења, можеме да го минимизираме ризикот и да уживаме во безбедно и одговорно онлајн искуство.

Ви благодариме на вниманието!