

Предавање - Заштита на идентитет во Интернет

Како што се зголемува процентот на популација што користи Интернет, така се зголемуваат и безбедносните ризици.

Кибертерациите станаа толку распространети што федералната влада на САД спроведе оддел за истражување и развој дизајниран да формулира план за развој на технологија и креирање политики кои ги минимизираат потенцијалните ризици во сајбер просторот.

Со зголемувањето на употребата на страниците и мрежите на социјалните медиуми, луѓето ставаат на располагање на повеќе лични информации на интернет светот, што го отежнува заштитувањето на вредните податоци. За среќа, постојат различни начини да се заштити сопствениот идентитет на Интернет и личните информации.

Еве ги првите 10 начини на кои можете да се заштитите преку Интернет:

1. Користете силни лозинки

Најчестиот начин да го заштитите вашиот идентитет на Интернет е да се фокусирате на создавање силни лозинки. Кога креирате лозинка, изберете нешто што нема лесно да се пробие или декодира. Никогаш не користете збор или број што некој може да го поврзе со вас, како што се име, средно или презиме, име на сопруга или дете, адреса, телефонски броеви, работодавци или други идентификувачки букви или броеви. Измешајте ги буквите и броевите користени во вашата лозинка и користете симболи и комбинација на големи и мали броеви кога е можно за да се заштитите од нарушувања на безбедноста на Интернет. Дополнително, важно е никогаш да не ја споделувате вашата лозинка со никого. Можеби е потребно да ги менувате вашите лозинки неколку пати годишно.

2. Побарајте шифрирање

Пред да направите каква било финансиска трансакција преку Интернет, побарајте знаци кои покажуваат дали веб-страницата е шифрирана или не. За да го направите ова, побарајте две работи: доверливи симболи за заклучување на безбедноста и дополнителни „и“ на крајот од http во лентата за URL или веб-адреса. Кога сте на страницата што бара информации за вашата кредитна картичка, „http“ се менува во „https“ кога е безбедна страница. Во исто време, симболот за заклучување исто така ќе се појави на десната страна од лентата за адреси или на долниот лев агол од прозорецот на вашиот прелистувач. Овие два сигнали покажуваат дека страницата е шифрирана, што значи дека

никој нема да може да гледа информации како што се испратени до сопственикот на веб-страницата. Ова ги чува вашето име, телефонски број, адреса, број на кредитна картичка и други чувствителни информации од видот на некој друг.

3. Инсталирајте Системи за безбедност

Безбедносните апартамани се безбедносни програми што ги спречуваат нечесните луѓе и програми да го заразуваат вашиот компјутер и да не крадат информации и податоци од вас. Ова вклучува блокирање на штетен софтвер, како што се шпионски софтвер, вируси и измами за фишинг, што може да се инсталира тајно кога сте онлајн. Некои од популарните безбедносни пакети вклучуваат антивирус Нортон, заштита од вируси Мекафи, безбедност на рекламирање и безбедност на Интернет АВГ. Бидете сигурни да купите и инсталирате еден од овие пакети за да ги заштитите вашите лични информации преку Интернет.

4. Вклучете ја црната листа на веб-прелистувач

Недостатокот на безбедност на Интернет делумно се должи на користениот интернет прелистувач. Многу веб-прелистувачи имаат дополнителни безбедносни опции како што е црната листа. Ова ви овозможува да ги поставите критериумите за страниците на кои ќе се движите; само безбедни, доверливи страници ќе бидат достапни за посета.

5. Избегнувајте измами за фишинг

Измामите за фишинг користат различни методи за да ги добијат вашите лични информации и да ви го украдат идентитетот. Постојат многу различни измами за фишинг, но може да се избегнат со едукација за тоа како да ги препознаете. За да избегнете жртва на измама за фишинг, никогаш не отворајте е-пошта или прилози кога испраќачот е непознат и не кликувајте на несигурни врски од чудни е-пошта. Дополнително, избегнувајте некој да нуди пари, непознати можности за работа или барања за донации во добротворни организации, бидејќи тоа може да биде заговор за добивање ваши лични информации и идентитет на Интернет

6. Добијте заштита на личните податоци

Друг начин да го заштитите вашиот идентитет на Интернет и чувствителните информации при нивно споделување преку Интернет е да добиете приватна заштита на податоците. Овој тип на безбедносен пакет ќе ги заштити сите приватни податоци што се вклучени во е-пошта, приватни програми за месенџер, страници за социјални медиуми или во разни блогови. Со вработување приватен пакет за заштита на податоци, дополнително можете да спречите хакери да ги собираат вашите лични податоци.

7. Заштитете го вашиот безжичен рутер со лозинка

Безжичен рутер кој пристапува на Интернет во вашиот дом или деловно работење, секогаш треба да биде заштитен со лозинка. Кога немате лозинка на вашата безжична мрежа, секој од вашиот опсег може да го користи и да пристапува до вашиот интернет, дури и хакер. Хакер со искуство во извршување на сајбер злосторства ќе го искористи ова во своја полза и ќе украде информации од вашиот компјутер додека пристапува на вашиот рутер. Исто така, треба да ја овозможите одликата за шифрирање на безжичниот рутер, кој ги меша сите податоци што ги испраќате на Интернет за дополнително да ги заштитите вашите чувствителни податоци.

8. Скријте ги вашите лични податоци

Можно е случајно да ги споделите вашите лични информации со други ако не го поставите правилно вашиот веб прелистувач. Секогаш кога ќе добиете нов компјутер или преземате и инсталирате нов прелистувач, прво можете да го конфигурирате. За да го направите ова, ќе пристапите до опцијата "поставување" на прелистувачот и изберете да го конфигурирате прелистувачот да не ги открива вашето име, адреса за е-пошта или други информации. Обавезно преземете го овој дополнителен чекор кога преземате или инсталирате прелистувач за да ја осигурите вашата приватност и безбедност.

9. Овозможете колачиња на вашиот веб-прелистувач само кога е потребно

Друга опција за поставување на вашиот прелистувач за заштита на вашите податоци на Интернет е овозможување колачиња само кога тоа го бара веб-страница. Овие колачиња се детали што веб-страниците ги чуваат на вашиот компјутер, вклучувајќи информации за тоа кои страници ги посетувате и што правите таму. Повеќето ги чуваат деталите за себе, но ова е и начин на кој нечесните луѓе ги добиваат вашите информации. Сакате колачињата да бидат овозможени, но да ги ограничувате само на веб-страници што ги бараат.

10. Заштитете ги информациите за вашата кредитна картичка

Друга опција за поставување на вашиот прелистувач за заштита на вашите податоци на Интернет е овозможување колачиња само кога тоа го бара веб-страница. Овие колачиња се детали што веб-страниците ги чуваат на вашиот компјутер, вклучувајќи информации за тоа кои страници ги посетувате и што правите таму. Повеќето ги чуваат деталите за себе, но ова е и начин на кој нечесните луѓе ги добиваат вашите информации. Сакате колачињата да бидат овозможени, но да ги ограничувате само на веб-страници што ги бараат.

Заработувајќи диплома за компјутерска безбедност е најдобриот начин да научите стратегии за да се заштитите од најновите закани во оваа дигитална ера.