ПРОЕКТ
ДИГИТАЛЕН ДОСТЪП
(*DIGITAL ACCESS PROJECT*)

УЧЕБЕН МОДУЛ
Напреднали знания за онлайн безопасност

Изготвил: AKLUB
Септември 2018

Този проект е финансиран с подкрепата на Европейската комисия. Тази публикация и цялото й съдържание отразяват само възгледите на автора и Комисията не носи отговорност за каквото и да е използване на съдържащата се в нея информация.

Съдържание

РЕЗЮМЕ ..... **Error! Bookmark not defined.**

РАЗДЕЛ 1- Защита на интернет мрежата *6*

Домашна безжична мрежа ..... ***Error! Bookmark not defined.***

Стъпка 1. Сменете името на вашата домашна мрежа 7

Стъпка 2. Уверете се, че слагате сложна и уникална парола, за да защитите вашата безжична мрежа 7

Стъпка 3. Засилване на вашата Wi-Fi сигурност чрез активиране на мрежово криптиране 8

Стъпка 4. Изключете безжичната домашна мрежа, когато не сте у дома 8

Стъпка 5. Къде се намира рутера във вашия дом? 9

Стъпка 6. Използвайте сигурна парола на администратор, за да засилите сигурността на вашата безжична мрежа 9

Стъпка 7. Промянете IP адреса по подразбиране на безжичния рутер 9

Стъпка 8. Изключете DHCP функционалността на рутера 10

Стъпка 9. Деактивирайте отдалечения достъп 10

Стъпка 10. Винаги поддържайте софтуера на рутера си актуализиран 10

Стъпка 11. Защитната стена може да помогне за защитата на Wi-Fi мрежата 11

Стъпка 12. Подобрете защитата на устройствата, които най-често са свързани към домашната ви мрежа 11

Заключения ..... ***Error! Bookmark not defined.***

Инсталирайте антивирусна програма ..... **Error! Bookmark not defined.**

Избягвайте подозрителни уебсайтове ..... **Error! Bookmark not defined.**

Никога не отваряйте прикачени файлове, без да ги преглеждат 13

Настройване на автоматични сканирания 13

Наблюдавайте всичко, което изтегляте от интернет ..... **Error! Bookmark not defined.**

Актуализирайте, Актуализирайте, Актуализирайте! 14

Винаги бъдете информирани ..... **Error! Bookmark not defined.**

Избягвайте „кракнат“ софтуер ..... **Error! Bookmark not defined.**

Инсталирайте защитна стена ..... **Error! Bookmark not defined.**

Бъдете подготвени ..... **Error! Bookmark not defined.**

Защита срещу зловреден софтуер ..... ***Error! Bookmark not defined.***

Инсталиране на анти-шпионски софтуер ..... **Error! Bookmark not defined.**

Как всъщност изглеждат имейлите със зловреден софтуе 22

ДОПЪЛНИТЕЛНА ИНФОРМАЦИЯ И РЕСУРСИ.....22

ЧАСОВЕ ЗА ОБУЧЕНИЕ: [ВСИЧКИ УЧЕБНИ ЧАСОВЕ]
НАТОВАРВАНЕ: [ВСИЧКИ УЧЕБНИ ЧАСОВЕ + ВРЕМЕ ЗА УПРАЖНЕНИЯТА]

РЕЗЮМЕ

Този модул е предназначен за разширяване на основните потребителски познания за онлайн безопасност, които се използват, насочен към начинаещи потребител на интернет. Основните цели на са да се даде възможност на потребителя да се предпази от кибер престъпници и да пази личната информация в безопасност, гарантираща, че неговите онлайн данни и активи не са компрометирани.

КЛЮЧОВИ ДУМИ

Домашна безжична мрежа, антивирусна програма, вирус, зловреден софтуер, шпионски програми, шпионски софтуер.

ЦЕЛ НА МОДУЛА

Дейности / Резултати		
Придобиване на разбиране за основани на интернет престъпни дейности, насочени към физически лица, и придобиването на умения за идентифициране и избягване на тези дейности.		
Знания	**Умения**	**Компетентности**
Обезопасяване на интернет връзки	Разбиране на домашната безжична мрежа Да умеете да я настроите Да знаете правилата за безопасност	Да можете да настройвате и управлявате сигурността на домашната безжична мрежа
Антивирусни програми	Разбиране на целта на вирусите и нуждата от антивирусни програми Да умеете да избирате най-подходящата антивирусна програма Да знаете как да избягвате вируси	Да знаете как да защитите вашия компютър срещу вируси.

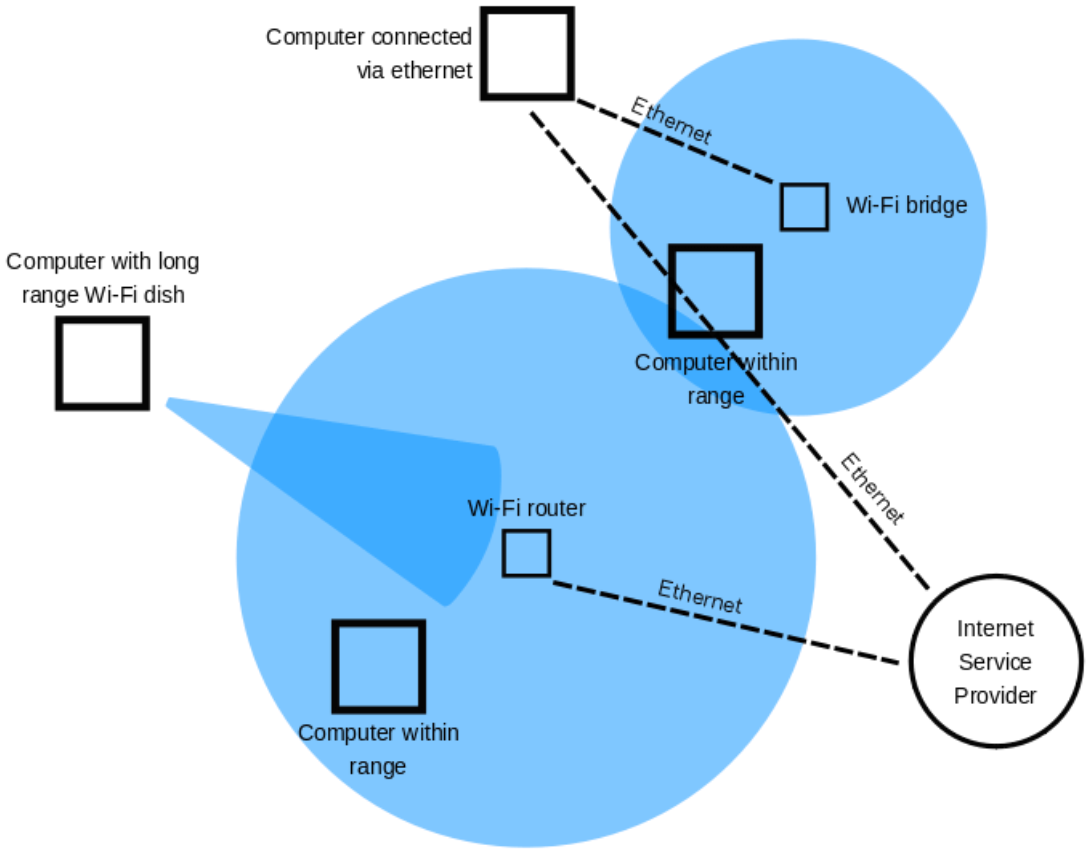
Зловреден софтуер	Разбиране на зловреден софтуер и нужда от програми срещу зловреден софтуер. Да може да избирате подходящи програми срещу зловреден софтуер. Да знаете как да предпазите вашия компютър от зловреден софтуер.	Да знаете как да предпазите вашия компютър от зловреден софтуер.

РАЗДЕЛ 1- Защита на интернет мрежата

Домашна безжична мрежа

С няколко прости думи, основната домашна безжична мрежа означва, свързване на точката за достъп до интернет, като например кабел от вашия интернет доставчик, към (безжичен) рутер, за да позволите на няколко устройства да се свързват с мрежата много бързо.

В много случаи след като веднъж безжичният рутер е бил инсталиран, намираме му място някъде в дома и забравяме за него. След като веднъж сме го свързали с интернет, свързването е през Wi-fi мрежа, и това е всичко, което има значение, нали? Погрешно!



Може би много от вас не осъзнават, но рутерът е едно от най-важните устройства в нашия дом. Той е пътя към достъпа до интернет и също така може да се използва от киберпрестъпници, които могат да се промъкнат в нашите устройства и да получат достъп до нашата система.

Единствената мярка, която повечето хора използват за защита на домашната си мрежа е да сложат парола и да попречат на съседите или другите хора да вземат контрол върху вашите

данни. Но трябва да се подходи по-сериозно за сигурността. Сериозният риск е, че един онлайн престъпник може да използва лошите ви мерки за защита на Wi-Fi и да "слуша" трафика ви, за да извлече чувствителна информация или да се възползва от вашата мрежа, за да стартира зловредени атаки като или кражба на данни и др.

Въпреки, че е относително лесно за използване и достъп, Wi-Fi мрежите не винаги са защитени. Wi-fi идва с много въпроси, свързани със сигурността, и си струва да се напомни за уязвимостта на крак (krack), открита в протокола за Безжичен Защитен Достъп II (Wireless Protected Access - WPA2), който засяга всички устройства, свързани чрез Wi-Fi.

По тази причина, научаването на това как да се защити домашната безжична мрежа срещу кибер престъпници е разумно решение.

Като се има предвид колко интернет на нещата (IoT) устройства може да притежавате, като се уверите, че вашата мрежа е допълнителен сейф носи още по-голяма тежест, въпреки, че понякога се грижи за вашата киберсигурност може да бъде досаден, но е нобходим.

В този урок ще научите как можете по-добре да защитите домашната си мрежа и да намалите шансовете за компрометиране на ценните ви данни.

Стъпка 1. Сменете името на вашата домашна мрежа

Ако искате по-добре да защитите по-добре домашната си мрежа, първото нещо, което трябва да направите, е да промените името на вашата Wi-Fi мрежа, известна още като SSID (идентификатор на сервизен набор).

Ако сложите на вашия Wi-Fi по-провокативно име, като например "Не може да хакнете този" може да се обърнете към други имена като "това не е WiFi" или "твърде готин за WiFi" , които са напълно приемливи.

Променяне на името на Wi-Fi по подразбиране го прави по-трудно за зловредени атаки да разберат какъв вид рутер имате. Ако кибер престъпниците знаят серийния номер на рутера, те ще знаят колко уязвим е моделът, който имате и по този начин може да го експлоатира.

Много е важно да не си кръщавате домашната WiFi мрежа с имена от рода на “Wi-Fi на Джон”. Вие нямате интерес те да знаят от пръв поглед коя безжична мрежа е вашата, когато има вероятно три - четири други мрежи на ваши съседи.

Също така имайте предвид, че споделянето на прекалено много лична информация на името на вашата безжична мрежа може да ви изложи на опасност от кражба на идентичност.

Ето и ръководство стъпка-по-стъпка, което показва как лесно може да смените името на вашата мрежа.

Стъпка 2. Уверете се, че слагате сложна и уникална парола, за да защитите вашата безжична мрежа.

Вероятно знаете, че всеки безжичен рутер идва предварително настроен с потребителско име и парола по подразбиране, която е необходима на първо място, за да инсталирате и свържете вашия рутер. Лошото е, че това е лесно за хакери да го стигнат до вашата парола, особено ако познават производството.

Така, че уверете се, че веднага след инсталирането на рутера сте сменили името и паролата.

Добре защитената парола трябва да бъде поне 20 символа дълга и да включва номера, букви и символи.

Използвайте това ръководство, за да настроите надеждна парола за вашата мрежа. Когато приятелите идват за посещение може да се оплакват от необичайната дължина на паролата си, но това може да ги обезкуражи от ненужно да използват вашите данни със скучни Facebook или Instagram постове.

Стъпка 3. Засилване на вашата Wi-Fi сигурност чрез активиране на мрежово криптиране

Безжичните мрежи се предлагат с няколко езика за шифроване, като WEP, WPA или WPA2.

За да разберете по-добре тази терминология, WPA2 стои зад Wi-Fi защитен достъп 2 и е както протокол за сигурност, така и текущ стандарт в индустрията (WPA2 мрежите са почти навсякъде) и криптира трафика на Wi-Fi мрежи. Той също така замества по-стар и по-малко защитен WEP (кабелна еквивалентна поверителност) и е ъпгрейд на оригиналната технология WPA (Wi-Fi защитен достъп) технология. Това е така защото от 2006 всички Wi-Fi сертифицирани продукти трябва да използват WPA2 сигурност.

WPA2 AES също е стандарт система за сигурност сега, така че всички безжични мрежи са съвместими с него. Ако искате да активирате WPA2 шифроването на безжичния рутер, използвайте тези шест стъпки. Ако използвате безжичен рутер TP-Link, Ето как да защитите вашата безжична мрежа.

Добрата новина е, че WPA3 е вече тук и ще замени WPA2. Този Wi-Fi алианс наскоро обяви стандарта си за защита на безжичната мрежа от следващо поколение, който има за цел да реши общ проблем със сигурността: отворени Wi-Fi мрежи. Повече от това, тя идва с подобрения в защитата и включва пакет от функции, за да се опрости Wi-Fi защитната конфигурация за потребители и доставчици на услуги.

Стъпка 4. Изключете безжичната домашна мрежа, когато не сте у дома

С цел да подсигурите вашата мрежа, силно препоръчваме да изключите безжичната си мрежа, в период в който за по-дълго време няма да го използват Ethernet кабели или когато не сте си вкъщи.

Като правите това, затворете всички прозорци и възможности за хакване, или за пробив докато отсъствате.

Ето няколко предимства от спирането на вашата безжична мрежа:

- **От гледна точка на сигурността** – Изключването на мрежовите устройства, намалява шансовете да станете мишена за хакери.
- **Защита от пренатоварване** – Когато изключите мрежовото устройство, можете също да намалите опасността от пренапрежение на електрическата енергия;
- **Намаляване на шума**– Въпреки, че съвременните домашни мрежи са много по-тихи тези дни, блокирането на безжичната домашна мрежа, може да добави спокойствие към дома ви.

  Въпреки, че съвременните домашни мрежи са много по-тихи тези дни, спирането на безжичната домашна мрежа може да добави спокойствие към дома ви.

Стъпка 5. Къде се намира рутера във вашия дом?

Вероятно не сте мислили за това, но мястото където се намира вашият рутер има връзка с вашата сигурност.

Сложете безжичния рутер колкото се може по-близо по средата на вашата къща. На първо място това се прави, за да се осигури равен достъп до интернет до всички стаи във вашия дом. На второ място не искате обхватът на безжичния сигнал да достигне твърде много извън дома ви, където може лесно да бъде хванат от зловредени лица.

По тази причина ние ви препоръчваме да не поставяте рутера си близо до прозорец, тъй като така няма нещо масивно, което да блокира сигнала, който идва от дома ви.

Стъпка 6. Използвайте сигурна парола на администратор, за да засилите сигурността на вашата безжична мрежа

За да настроите безжичния рутер, обикновено трябва да осъществите достъп до онлайн платформа или сайт, където можете да направите няколко промени в мрежовите настройки.

Повечето Wi-Fi рутери идват с идентификационни данни по подразбиране като "администратор" и "парола", които са много лесно за зловредени хакери да влязат.

Знаете ли, че броят на безжичните мрежи се е увеличил драстично през последните 8 години? В 2010 имаше 20 000 000 Wi-Fi мрежи по целия свят, и за 8 години, този брой се увеличил до 400 000 000.

Стъпка 7. Промянете IP адреса по подразбиране на безжичния рутер

Промяната на IP адреса по подразбиране е друго нещо, което трябва да обмислите, за да защитите по-добре домашната си мрежа и да я направите по-трудна за проследяване от хакери.

За да промените IP адреса на рутер, трябва да следвате тези стъпки:

1. Влезте в конзолата на рутера като администратор. Тези основни стъпки ще ви научат как лесно да се свържете до домашната ви мрежа, като администратор. Обикновено адреса се изписва по следния начин: http://192.168.1.1 or http://192.168.0.1
2. След като веднъж влезнете, въведете потребителско име и парола на страницата за регистрация;
3. После изберете „Мрежа“ > LAN, която е в менюто от лявата страна;
4. Сменете IP адреса за предпочитане, след което килнете „Запамети“.

Забележка: След като промените IP адреса, ще трябва да въведете новия IP адрес в уеб браузъра.

Можете също да промените DNS сървъра, който безжичният рутер използва за филтриране на интернет трафика, и този урок ще покаже как да го направите.

Стъпка 8. Изключете DHCP функционалността на рутера

За да се засили сигурността на уайърлес мрежата, трябва да изключите сървъра за динамичен протокол за конфигуриране на хост (DHCP) във вашия рутер, което е това, което IP адресите са причислени на всяко устройство в мрежа. Вместо това трябва да използвате статичен адрес и да въведете мрежовите настройки. Това означава, че трябва да влезете в устройството си и да му приспособи към IP адрес, който е подходящ за вашия рутер.

Стъпка 9. Деактивирайте отдалечения достъп

Повечето рутери ви позволяват достъп до техния интерфейс само от устройства, свързани с интернет. Въпреки това някои от тях позволяват достъп дори от разстояние.

След като изключите отдалечения достъп, зловредените няма да могат да получат достъп до настройките за поверителност на от устройство, което не е свързано към безжичната мрежа.

За да направите тази промяна, достъп до уеб интерфейса и търсене на "отдалечен достъп" или "отдалечена администрация".

Стъпка 10. Винаги поддържайте софтуера на рутера си актуализиран

Софтуерът е съществена част от сигурността на безжичната мрежа. Фърмуера на безжичния рутер, като всеки друг софтуер, съдържа недостатъци, които могат да станат много уязвими от хакери.

За съжаление, много безжични рутери не разполагат с опцията за автоматично обновяване на софтуера, така че трябва да преминете през неудобството да правите това ръчно.

И дори за тези Wi-Fi мрежи, които могат да се актуализират автоматично, той все още изисква да включите тази настройка. Но ние ви напомняме за важността на софтуерните корекции и как пренебрегването на това може да остави отворени врати за кибер престъпниците да използват различни вратички. Прочетете какво казват експертите по сигурността относно актуализирането на софтуера и защо той е ключ към онлайн сигурността.

Стъпка 11. Защитната стена може да помогне за защитата на Wi-Fi мрежата

Защитата не са само софтуерни програми, използвани на вашия компютър, те също идват в сорта на хардуера.

Най-добрата част за хардуерните защитни стени е, че повечето от най-добрите безжични рутери имат вградена защитна стена, която трябва да защитава вашата мрежа от потенциални кибератаки. Този урок може да ви помогне да разберете дали вашият рутер има вградена защитна стена и как можете да я активирате. И ние силно препоръчваме да го включите, ако това не е по подразбиране като допълнителна защита.

Ако вашият рутер няма такава, можете да инсталирате добра защитна стена на рутера си, за да защитите системата си от зловредени опити за хакване срещу домашната ви мрежа.

Стъпка 12. Подобрете защитата на устройствата, които най-често са свързани към домашната ви мрежа

Важно: Не оставяйте неща, изложени на опасност от кибер престъпници!

Въпреки че сте увеличили защитата за вашия рутер в домашна мрежа, трябва да се уверите, че не разполагате с никакви пропуски по отношение на сигурността, които могат да бъдат използвани от онлайн престъпници.

Ето какво ви препоръчваме да направите:

1. Не забравяйте винаги да поддържате вашите устройства актуализирани с най-новия софтуер;
2. Винаги прилагайте най-новите корекции на сигурността, за да се гарантира, че няма пропуски в сигурноста за зловредени хора.
3. Проверете кои устройства се свързват най-често към вашата домашна мрежа и се уверете, че те имат антивирусен софтуер за защита срещу зловреден софтуер. Ако не знаете коя от тях трябва да изберете, това ръководство ще бъде много полезно.

4. Уверете се, че да защитите вашите устройства с помощта на множество системи за сигурност, състоящите се от специализиран софтуер за сигурност, като например актуализирани антивирусни програми и софтуер за филтриране на трафика. Можете да обмислите използването на софтуерна програма.

Заключения

Гарантирането на домашната мрежа трябва да бъде първостепенен приоритет за всеки от нас, който се интересува от запазването на данните безопасни и сигурни. Тези стъпки могат да бъдат наистина полезни дори и за технически неграмотен човек.

Също така, не забравяйте, че сигурността на безжичната мрежа може да бъде понякога слаба и склонна към експлоатиране. Почти няма значение колко силна е вашата парола или ако вашият софтуер е актуализиран, киберпрестъпниците могат просто да отвлекат вашите Wi-Fi данни.

РАЗДЕЛ 2: Антивирусни програми

Резултат

Повечето системи се нуждаят от антивирусен софтуер. Ето какво да изберете, как да го инсталирате, как да го използвате, за да бъдете сигурни.

Вируси

Това е нещо, което всички ние се стремим да избягваме, но истината е, че не можем винаги да го избегнем. Някои от нас имат лошия късмет да хванат компютърен вирус. Спазването на правилата ви помага да сведете до минимум.

Инсталиране на антивирусна програма

Независимо дали сте свързани с интернет или не, надеждната защита е правилния път. Антивирусните програми изискват минимална инвестиция и си струват парите, така, че след като си пуснете компютър, проверете дали сте добре защитени! В този урок можете да намерите връзка към отзиви за антивирусен софтуер. Можете да избирате от безплатни и платени оферти, изберете най-подходящата за вас антивирусна програма и може да я инсталирате директно самия уебсайт.

Избягвайте съмнителните уебасйтове

Много пъти уебсайтовете ще ви уведомят, ако сте на път, който се опитва да инсталира и изпълнява програма на вашия компютър, но не винаги. Избягвайте такива уебсайтове.

Никога не отваряйте прикачени файлове без преди това да им направите сканиране за вируси

Най-честият начин вирусите да се разпространяват остава е чрез електронната поща. Убедете се, че използвате имейл доставчик, който сканира всички качени файлове за вируси преди отварянето им, за да гарантира, че компютърът ви няма да получи вирус.

Настройване на автоматични сканирания

Настройването на сканирания, които да се изпълняват на компютъра ви ежедневно или ежеседмично, е добре, тъй като ще ви предпази от вируси. Това поддържа вашия компютър актуализиран и изчистен.

Наблюдавайте всичко, което изтегляте от интернет

Разбираме, че изтеглянето на музика и филми от интернет е масово и всеки го прави, но е хубаво да се знае, че това не представлява заплаха за вашата сигурност. Големите файлове, които изтегляте носят големи рискове.

Актуализирайте, Актуализирайте, Актуализирайте!

„Критичната актуализация“ на Майкрософт е чудесен пример за превенция от хакерски атаки. Неговата функция е да държи компютъра ви незасегнат от компютърни вируси. Винаги си актуализирайте системите.

Винаги бъдете информирани

Независимо дали сте компютърън маняк или просто използвате вашия компютър, за да работите на него, винаги бъдете информирани кое как ще се отрази на вашия компютър. Това ще ви подготви, ако нещо се случи да можете да установите и поправите проблема по-рано.

Избягвайте „кракнат“ софтуер

Всеки знае, че можете да изтеглите незаконен или „кракнат“ софтуер, което е по-евтиния вариант, но на практика изтеглянето на такива програми ви засяга компютъра. Те подлагат компютъра ви на трудни за откриване бъгове, и в крайна сметка ще ви причинят повече проблеми.

Инсталирайте защитна стена

Защитната стена е програма, която сканира входящия интернет и мрежовия трафик. Заедно с вашата анти-вирусна програма, тя може да помогне за предотвратяване на неоторизиран достъп до вашия компютър.

Бъдете подготвени

Ако имате някакви съмнения за вирус, който върлува, трябва да се убедите, че сте високо защитени. Не изтегляйте нищо и бъдете свръх предпазливи, когато отваряте имейли.

Този раздел трябва да ви помогне да се подготвите за всякакви компютърни вируси, които могат да ви се изпречат. Не забравяйте винаги да бъдете внимателни и предпазливи, когато използвате компютъра си!

РАЗДЕЛ 3:
Зловреден софтуер

Резултат

Идентифициране и справяне с киберпрестъпленията и възможностите за докладване

Зловреден софтуер / Malware/

Malware /Зловреден софтуер/, комбинация от думите *malicious* и *software* се отнася за тип компютърна програма, предназначена да зарази един законен потребител на компютъра и да нанесе вреда върху него по няколко начина. Malware може да зарази компютри и устройства по няколко начина и идва в редица форми, само някои от които включват вируси, червеи, троянски коне, шпионски софтуер и др. Жизнено важно е всички потребители да знаят как да разпознават и да се предпазват от зловреденрен софтуер във всички негови форми.

И така, какво е зловреден софтуер? Компютърните вируси са вероятно най-познатия тип зловреден софтуер — така наименувани, защото те се разпространяват, като правят копия от себе си. Червеите имат подобни свойства. Другите видове зловреден софтуер, като например шпионския софтуер, са наречени за това, което правят: в случай на шпионски софтуер той предава лична информация, като например номера на кредитни карти.

Защитата на вашия компютър и лични устройства от зловреден софтуер изисква както текуща лична бдителност, така и помощ от професионалните компании за сигурност. В днешно време, зловреден софтуер не просто прониква във вашите домашни компютри, но също така и мобилните устройства, които вие и вашето семейство използвате. И проблемът е по-голям, отколкото си предполагате.

Можете да бъдете жертва на злонамерена атака, чрез вашите уеб браузъри, имейли, социални мрежи и изтеглени файлове.

Вашето устройство може да бъде заразено чрез почти всеки онлайн процеси или дори USB флаш памет на ваш приятел, така че е важно да се използва програма за сигурност, която може да осигури пълна активна защита, което ви помага, преди да се заразят.

Така че след като попитат “казва се зловреден софтуер? " следващите логически въпроси са, "кой го създава, и защо? " дните, когато повечето зловреден софтуер е създаден от тийнейджърите, са отдавна отминали. Malware днес е до голяма степен проектирана от и за професионални престъпници.

Тези престъпници могат да използват различни сложни тактики. В някои случаи, като отбелязва технологичният сайт Public CIO, киберпрестъпниците дори "заключват" компютърни данни – което прави информацията недостъпна – след това ви иска откуп, за да получите тези данни обратно.

Но основният риск от кражбата на онлайн банкова информация като банкови и кредитни карти сметки и пароли. Хакерите, които крадат тази информация, може да го използват, за да източат сметката ви например. Или могат да продадат информацията за профила ви на черния пазар, където тази поверителна информация струва скъпо.

Защита срещу зловреден софтуер

И така най-важния въпрос за всички: "Как да се уверя, че моят компютър или мрежа е защитена от зловреден софтуер? "

Отговорът има две части: лична бдителност и инструменти за защита. Един от най-популярните начини за разпространяване на зловреден софтуер е по електронна поща, която може да бъде, за да изглежда така, сякаш е от позната компания, като например банка, или личен имейл от приятел.

Отговора също има две страни: Лична бдителност и инструменти за защита. Един от най-популярните начини за разпространение на зловреден софтуер е по имейл, която може да бъде маскиран да изглежда така, сякаш е от позната компания, като например банка, или личен имейл от приятел.

Бъдете предпазливи спрямо имейли, от някой, който иска да си представите паролата. Или имейли, които изглеждат сякаш са от ваши познати или приятели, но имат само едно съобщение, като например "Вижте този готин сайт! ", последвано от връзка.

Лична бдителност е първият етап на защита срещу зловредният софтуер, но просто да внимавате не е достатъчно. Понякога дори да изтегляте от легални няма гаранция, че сте защитен от зловреден софтуер. Което означава, че дори и най-разумният потребител е в опасност, освен ако не предприемете допълнителни мерки.

Инсталиране на анти-шпионски софтуер

Шпионският софтуер е софтуерна програма, която събира лична информация. Тази информация е пренасочена към уебсайт от трета страна. Шпионският софтуер е проектиран така, че да не е лесно да бъде проследен. Анти-шпионския софтуер е създаден да се бори

срещу шпионският. Подобен на антивирусния софтуер, анти-шпионския софтуер предлага защита в реално време.

Той сканира цялата входяща информация и помага за блокирането на заплахата, след като бъде открита.

Анти-шпионски софтуер можете да намерите в края на урока. Можете да изберете най-подходящия за вас.

Защитата не е абсолютна. Но комбинацията от лично съзнание и добре разработени защитни инструменти ще направят компютъра ви толкова безопасен, колкото може.

УПРАЖНЕНИЯ

Упражнение 1: Поемете контрола на вашия рутер чрез уникална парола:

Стъпка 1: Свържете се към вашия безжичен рутер.

Отворете „Internet Explorer“ и въведете адреса http://192.168.0.1 or http://192.168.1.1 (По подразбиране, повечето рутери ще започват с **192.168**.0.1 или **192.168**.**1.1** като IP адрес по подразбиране на рутера. Това е адреса, който ще въведете във вашия браузър за достъп до конфигурационната страница на рутера.)

Сега влезте в рутера. Какво??. Нямате потребителско име и парола??. Не се безпокойте. Той разполага с идентификационни данни (при условие, че не сте го променили по-рано)

Потребителското ви име и парола трябва да бъдат:

Пет символа. Всичките малки. 1-ва азбука, а след това четвъртата азбука, 13-та азбука, а след това 12-та азбука, тогава 14-та азбука.

За ваше улеснение:

Потребителско ID: admin

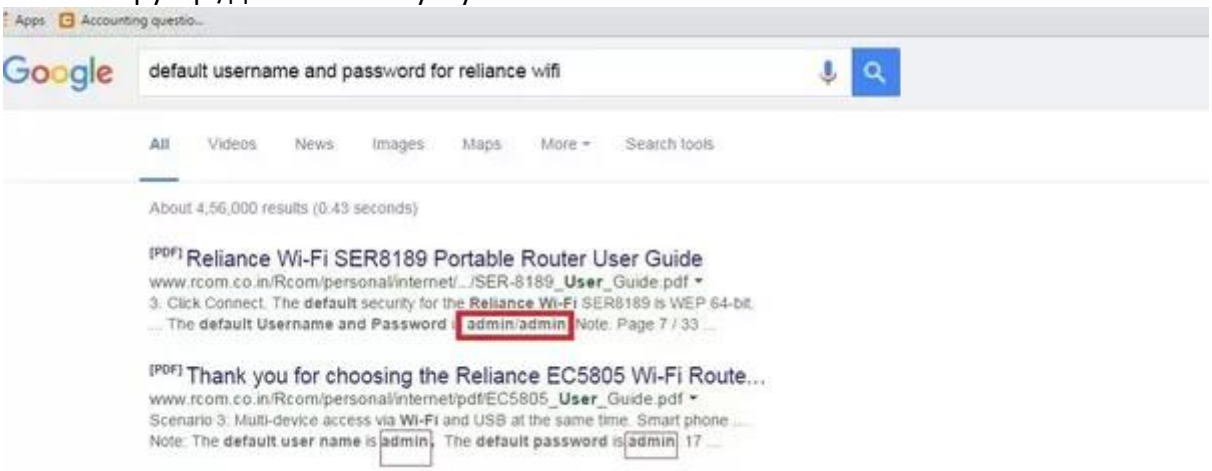
Парола: admin

или

ID на потребителя: admin

Парола (празно):

Ако не работи за вас, моля въведете в google потребителско име/парола по подразбиране за вашия рутер /доставчик на услуги.

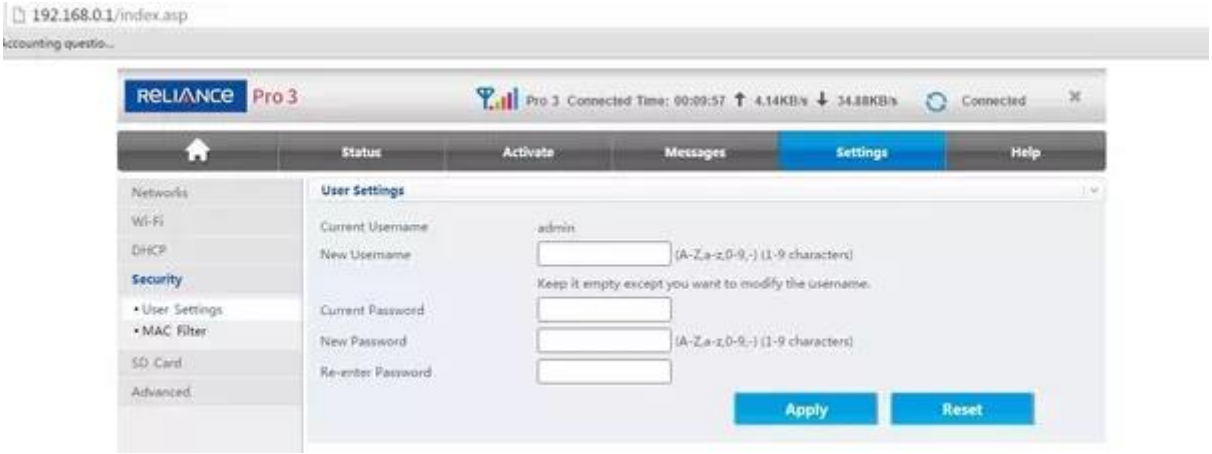


Стъпка 2: Променете потребителското си име и паролата незабавно.

- Отидете в настройките

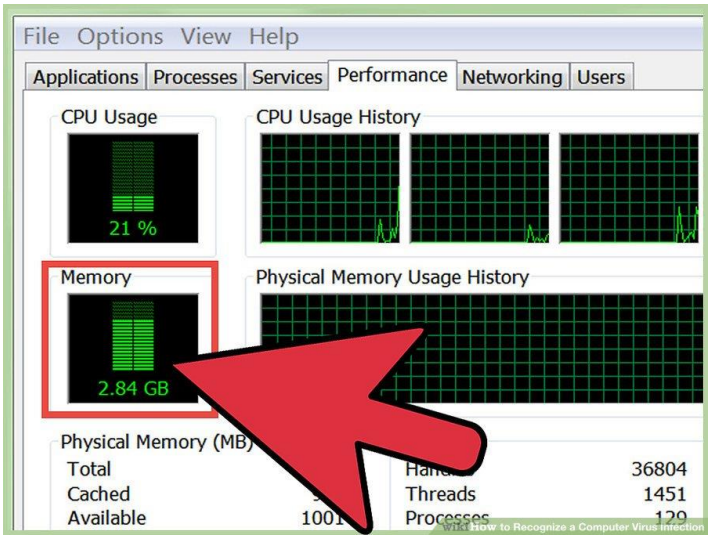
- Потребителски настройки

- Актуализиране на новите ви идентификационни данни



Упражнение 2: Разпознаване на вирус на вашия компютър

1. Проверка на активността на хард диска. Ако не използвате никакви програми и светлината на хард диска постоянно се изключва или го чувате да работи, може да имате вирус, който работи във фонов режим.



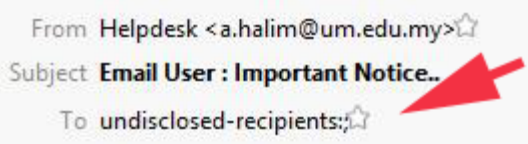
2. Засечете колко време отнема на компютъра ви да зареди. Ако започнете да забелязвате, че компютърът ви отнема значително повече време от обичайното за стартиране, вирусът може да забави процеса на стартиране.

Ако не можете да влезете в Windows, вирусът най-вероятно влияе върху процеса на влизане.

3. Вижте светлините на модема ви. Ако светлините за прехвърляне на модема ви постоянно мигат, може да имате вирус, който предава данни по мрежата.

Упражнение 3: Разпознаване на зловреден софтуер имейл

1. **Имейл адреса на подателя**. Ако адресът на подателя е непознат или не съвпада с очакван адрес за фирма, то вероятно е имейл със злонамерен софтуер. Повечето злонамерени имейли изглеждат като уведомления за доставка на пратка, фактуриили съдебни уведомления. Такива имейли рядко идват от правилен адрес, като например имейли, които претендират, че са от DHL или UPS, вероятно са злонамерени, ако адресът не кореспондира с оригиналния адрес ups.com или dhl.com.
2. **Предмета или прикачените файлове съдържат потребителско име.** Имейл със злонамерен софтуер може да съдържа потребителското ви име в темата или името на прикачения файл или полето "относно" може да е празно. Контрастира това с нормалните имейли, които почти винаги има написана тема в относно.
3. **Изкушаване от отваряне на прикачените файлове.** Много имейли, съдържащи злонамерен софтуер, ще ви изкушава да отворите прикачения файл. Много прикачени файлове могат да бъдат вредни, дори ако използвате антивирусна програма. Имейлите, които са свързани с доставка на пратки нямат причина да ви приканват да отваряте файлове; дори да има някакъв проблем, той може да бъде описан в тялото на имейла.
4. **Изкушаване от отваряне на линк. Някои злонамерени имейли** са подобни на фишинг имейлите, където ви стимулират да последвате даден линк. Този линк може да доведе до зловреден софтуер, така че моля, обмислете първо всички рискове.
5. **Проверка на информацията.** Ако имейл ви иска да потвърдите, проверите, прегледате или предоставите информация с помощта на прикачен файл, той може да е прикачен към зловреден софтуер. Помислете дали това изглежда безопасно и се свържете с поддръжката, ако се съмнявате.
6. **Предупреждение за проблем, заплаха или спешност**. Злонамерените имейли често се опитват да ви накарат да се изплашите, да се разтревожите или да изпитате чувство на спешност. Ако имейлът ви насърчава да разрешите проблем, като отворите прикачен файл, трябва да бъдете много предпазливи. Някои имейли изглежда като втори отговор, който ви моли за последващи действия. Примерите включват справяне с проблеми при доставката на пратки, информация за фалшиви призовки и фалшиви фактури от лица, с които нямате бизнес.
7. **Неизвестни/скрити получатели.** Ако списъкът с получатели на имейли не е видим, това може да е злонамерен софтуер.



8. **Подозрителни прикачени файлове. Ако имейлът има неочакван прикачен файл с разширение** .doc, .zip, .xls, .js, .pdf, .ace, .arj, .wsh, .scr, .exe, .com, .bat, или друг вид файл на Microsoft Office , може да бъде злонамерен. Имайте пред вид, че понякога разширението на файла е скрито или съдържанието не отговаря.

9. **Обикновен текст/без лого.** Легитимните имейли обикновено са написани на HTML и и имат комбинация от текст и изображения. Злонамерените имейли рядко имат изображения и са с обикновено форматиране.
10. **Общ поздрав**. Ако имейлът е адресиран с общото "Уважаеми клиенти ", тогава може да е злонамерен софтуер или опит за фишинг.
11. **Неочаквано съдържание на прикачения файл.** Ако в крайна сметка отворите прикачен файл и съдържанието са празни или са много различни от това, което сте очаквали, може да е зловреден софтуер. Моля, свържете се с поддръжката за помощ веднага! Поддръжката може да ограничи щетите или да ви помогне да се възстановите.

Как всъщност изглеждат имейлите със зловреден софтуер?

Ето истинска снимка на пощенска кутия, съдържаща 19 имейла от зловреден софтуер:

Subject	Correspondents	Date
URGENT RFQ	AL WALEED EQUIPMENTS	03/13/2017 06:55
	starsescorts@gmail.com	03/15/2017 01:27
New Order Attached **KINDLY SEND INVOICE	Amr Hassan	03/15/2017 19:30
We're sad to let you know that our delivery was unusuccessful....	FedEx Expedited Express	03/16/2017 02:53
47929 username2	pkeith@gejlaw.com	03/16/2017 05:29
Delivery Status Notification	webmaster@stroy-exp...	03/16/2017 05:47
	vowsbyjudy@shaw.ca	03/16/2017 14:38
Formal Inquiry	"Anaïs VANACKER"<Va...	03/16/2017 21:16
We have delivery problems with your parcel #7104543	webmaster@whfarm2....	03/17/2017 00:57
INQUIRY	Saigon Offshore	03/17/2017 03:47
	dava@ac-lyon.fr	03/17/2017 14:25
54343 username	juanro5554@hotmail.c...	03/17/2017 14:48
Item Delivery Notification	alifeof8@server.alifeofj...	00:34
UPS courier can not deliver parcel #004287245 to you	webmaster@stroy-exp...	06:23
Parcel Delivery Notification	abidjanbateau@vps286...	06:52
Visa Card Award	info@visa.com	07:21
Problems with item delivery, n.4930349	Apache	09:54
Package Delivery Notification	Apache	10:06
Delivery Status Notification	contrav8@box980.blue...	17:05

Упражнение 4: Онлайн викторина за безопасност

Направете тази онлайн викторина и вижте

какъв е вашия резултат

https://www.proprofs.com/quiz-school/story.php?title=esafety-quiz

ДОПЪЛНИТЕЛНА ИНФОРМАЦИЯ И РЕСУРСИ

Условия, които трябва да знаете

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Интернет безопасностза възрастни хора (PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjAReqQIBxAC&url=https%3A%2F%2Fvictimserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSeniors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Топ съвети за интернет безопасност (PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjALegQIBRAC&url=https%3A%2F%2Fquery.prod.cms.rt.microsoft.com%2Fcms%2Fapi%2Fam%2Fbinary%2FRE1ImTu&usg=AOvVaw0QyXRMv5RLg-kAS0tIaUvz

Как да се предпазите от злонамерен

софтуер – Youtube видео

https://www.youtube.com/watch?v=uJRqZTNMC

Mo

Най-добрите антивирусни услуги за 2018 година

https://www.itproportal.com/guides/best-antivirus-services-for-2018/

Най-добрият антивирусен софтуер за 2018 година

https://www.techradar.com/news/best-free-anti-malware-software

Защита на данни

https://youtu.be/BL7WJM342Uc

Онлайн безопасност за възрастни хора

-

https://www.connectsafely.org/seniors/

Онлайн безопасност

https://www.protectseniorsonline.com/resources/

Как да проверите дали компютърът има вирус

https://www.youtube.com/watch?v=4i_cCPhewu4