Добре дошъл в <име тук>. Тук ще се научиш на някой от основните заплахи в интернет и как да се защитиш от тях.

Слабата парола

-Паролата е едно от най-важните неща в интернет и ти трябва да се погрижиш тя да е достатъчно сигурна и надеждна.

Когато влизаш в интернет, ще ти се налага да мислиш пароли за акаунтите, които създаваш. В интернет има правила, които е хубаво да се спазват, за да може паролата ти да не може да бъде отгатната от хората, които не искаш. Ето ги и правилата:

Паролата трябва да е съставена от:

- Главна и малка буква  
- Числа  
- Специални символи (!,@,№,$,%,€)

Един хубав пример за парола е: HawqkP4!#0n

...И един пример за лоша такава: 3245986miTko

Също така е много важно паролите ти да са различни за всеки сайт,защото някой може да се досети и да използва паролата ти от един сайт в друг и по случайност да уцели паролата ти и да влезе в твоя акаунт, а от там могат да настъпят проблеми.

Непознати източници

Понякога се случва да получиш някакво съобщение или файл от непознат човек. Този файл може да изглежда като съвсем нормален документ, но има голяма вероятност да съдържа вирус. Чрез отваряне на този файл, може да навредиш сериозно на устройството от което отваряш файла.

По много начини може да се разбере злонамерения подател, като например:  
- Странно име на подателя или непознат за теб подател.  
- Съмнително разширение на изпратения файл(разширение е това, което седи на края на името на файла, като .txt, .exe и т.н. Доста опасни са файловете с разширение .exe, .msi и .xml)  
- Имейл, който е от официален или дори известен сайт, но името е променено(силно опасно е да се отварят файлове от такива източници. Името трябва да съвпада с официалното и подателя да е с нормален имейл адрес.)

Фишинг атаки и изнудвачи

Фишинг атака е процес при който злонамерен човек ти праща файл, линк, някакъв вид документ, като целта му е отмъкване на информация от теб. Може да ти прати сайт, които много добре познаваш, за да видиш "интересна картинка", но преди да я видиш, да трябва да влезеш в профила си и точно така той взима паролата ти и името на акаунта. Изнудвачите са хора,които имат същата цел, но те говорят с теб, като използват заплашителни думи или изрази с които могат да те изплашат. Думите могат да бъдат от вида на: "Кажи ми къде живееш, да дойда да се видим", "Искаш ли да излезем по-късно да се запознаем","Знам къде живееш, така че не се опитвай да ме блокираш" "Много си хубава, може ли да ми дадеш номера си" и много други, като някой път могат да са по-сериозни, от типа на "Майка ми има нужда от операция, и ми трябват спешно пари, а аз няма откъде да намеря", като по този начин те се надяват ти да се хванеш и да изпратиш колкото пари измамника поиска. Да се защитим от такива атаки не е трудно.

Трябва да:

- Не отговаряш на непознати в интернет  
- Не вярваш на това какво ти казват  
- Съобщиш на възрастен и ако се налага да съобщиш в полицията.  
  
(Говорене в презенацията: Важно е да знаеш, че да говориш с непознати в интернет може да бъде наистина сериозно, тъй като някои изнудвачи са по-добри от други и могат да пробит защитата на компютра ти и да откраднат снимки или някои важни файлове. Ако случайно забележиш някаква странна дейност на компютъра си, най-доброто решение да издрпаш кабела на интернета. Така злосторника губи връзка с компютъра ти и няа опасност да разруши жизненоважни файлове за правилната работа на компютъра)

Уеб сайтове

Всеки уеб сайт си има някаква защита. Има обаче сайтове, който нямат такава и със тях трябва да се внимава. Накратко защитата на сайтовете може да се раздели на 4 - държавни/правителствени сайтове(те завършват на .gov или .edu), обикновени защитени сайтове, несигурни сайтове и опасни сайтове. Може би се чудите каква е разликата между несигурни и опасни сайтове - при несигурните сайтове, браузърът(Google, Yahoo, Mozilla Firefox) ти казва, че сайта няма защита, но не е опасен, докато при опасните сайтове, браузърът предупреждава, че сайта може да е потенциално опасен и ако влизаш, може вирус да се изтегли без да забележиш и устройството ти да стане по-бавно, затова за да се предпазиш, трябва да гледаш името на сайта, като следваш тези лесни стъпки:

- Сайта да започва с https, а не с http, защото http е несигурен сайт, но пък това не значи че на всяка цена би навредил. Все пак бъди предпазлив.  
- Ако името на сайта започва или завършва с нещо, което не ти е познато или дори не си го виждал, по-добре не работи с този сайт(кат например да завършва на .cf, .ga, .gq и др.).  
Рядко ще срещаш такива сайтове, но сайтовете с .edu или .gov(вместо .com) са най-сигурни.