Кирил Николов Киров

ПМГ „Акад.Боян Петканчин“ гр.Хасково

КАК ДА ИЗБЕГНЕМ КРАЖБА НА САМОЛИЧНОСТ И ДА СЕ ПРЕДПАЗИМ ОТ ФАЛШИВИ ПРОФИЛИ

Основен въпрос

Как да избегнем кражбата на самоличността ни в интернет и създаването от наше има на фалшиви профили?

Обзор на урока

Учениците научават, че сайтовете трябва да защитават тяхната лична информация. Те учат каква информация за себеси е безопасно да разпознават сайтовете.

Учениците обсъждат сценарий, самоличноста им в социалните млежи е откраднатa или е създаден фалшив профил с техни лични данни.Така те научават какво е поверителна информация и за законите за поверителност.

Цели на уроки

Учениците ще могат да:

- Научат каква информация трябва да избягват да споделят онлайн, защото е лична;
- Как да се предпазят от кражба на самоличността им в мрежата и злоупотреба с лични данни и снимки.
- Упражняват как да проверяват сайтовете, които посещават, дали имат политика на поверителност и поверителни печати на одобрение

Речник

Поверителна информация - информация, която може да бъде използвана, за да идентифицира – например - твоя ЕГН, домашен адрес, имейл, телефонен номер и т.н.

Кражба на самоличност– друг човек се представя в интернет от ваше име използвайки вашите лични данни и снимки.

Фалшив профил – профил в интернет който използва ваши данни и снимки, но под друго име.

Въведение

Кажи на учениите да си представят, че някой от тяхно име води лична кореспонденция например във фейсбук, туйтър или сайт за запознанства като използва личните им данни и снимки.

Попитай

Как бихте се чувствали?

Отговорите могат да бъдат – гневен, объркан, странно, неудобно, ОК

Ще се чувстваш ли по-добре, ако ти решаваш кой да знае такива неща за теб?

Учениците могат да искат да контролират кой да притежава информация за тях

Обсъдете с учениците факта, че личната информация не трябва да бъде споделяна с непознати и че известна информация – наречена поверителна информация- е особено важно да бъде защитена поради опасност за тяхната сигурност.

Определи понятието поверителна информация.

Тя включва: Пълно име, домашен адрес, име на училището и адрес, телефонен номер, емейл адрес, ЕГН, бакови сметки ,финансово състояние на семейството.

Основни методи за кражба на самоличност – 20 минути

- Разбиване на парола(хакване) за достъп до профили в социалните мрежи , електронно банкиране и други сайтове. Най-често се използват програми(вируси) прикачени към писма в ел.поща, към снимки или музикални файлове изпращани през личния чат на фейсбук, туйтър, скайп, месенджер и др.В резултат паролата се копира и в последствие променя от друг човек който получава контрол над профила.
- Създаване на профил с ваши данни и снимки непредпазливо публикувани или предоставени от вас самите.
- Създавани на фалшиви профили под други имена но със ваши снимки публикувани в сициалните мрежи.
- Последиците са кражби от банковите сметки , електронно пазаруване за ваша сметка или възможност за достъп до лични снимки и съобщения използвани в последствие за кибертормоз и уронване на доброто Ви име. Създавани на конфликти от ваше име с други учасници в мрежата.

Методи за предпазване-дискусия – 20 минути

Учениците на база на наученото в часовете по информатика и собствения си опит дискутират върху това как да се предпазят от кражба на самоличност . Рузултатите се сравняват с ПРИЛОЖЕНИЕ Интернет и децата -Докато работиш в интернет.

Заключителна част

Може да използваш въпросите по-долу, за да оцениш доколко учениците са разбрали целите на урока.

Какви примери на поверителна информация може да дадете?

Примери включват – имена, домашен адрес, име и адрес на училището, телефонен номер, емейл адрес и ЕГН.

Защо не трябва да споделяш своята поверителна информация?

Защото информацията може да бъде използвана от непознати. отделни личности или компании, за да ви потърсят и да установят контакт.

ПРИЛОЖЕНИЕ Интернет и децата
Докато работиш в интернет,

1. Не давай лична информация като име, парола, адрес, домашен телефон, месторабота и служебен телефон на родителите си или училището, в което учиш.
2. Не изпращай свои снимки или снимки на твои близки, без преди това да си обсъдил решението си със своите родители.
3. Винаги преди да качиш своя снимка и/или да публикуваш своя мобилен номер, помисли добре дали искаш и ще е добре ли за теб тази информация да стане достъпна за един неограничен кръг от хора.
4. Не приемай среща с някого, с когото си се запознал в интернет, без знанието на твоите родители. Ако те одобрят срещата, нека тя да е на публично и оживено място и задължително да е в присъствие на твои близки или приятели.
5. Не отговаряй на съобщения, които са обидни, заплашващи, неприлични или те карат да се чувстваш неудобно. Информирай родителите си или друг твой близък възрастен човек за такива съобщения и за техния източник.
6. Не отваряй приложения на електронна поща, получени от непознат подател. Те могат да съдържат вирус или програма, която да увреди твоя компютър или да черпи неограничено информация от него.
7. Внимавай, когато някой ти предлага нещо безплатно или те кани да се включиш в дейност, обещаваща лесна, бърза и голяма печалба. В тези случаи, най-вероятно, ще станеш жертва на измама.
8. Бъди внимателен и наблюдателен при попълване на регистрационните форми при извършване на регистрация в интернет сайтове.
9. При регистрации винаги проверявай има ли данни на сайта относно администратора/модераторите, които го поддържат, както и възможност за обратна връзка с тях – адрес за контакт.
10. Чети „Условията за ползване” на сайта, преди да се съгласиш с тях! Там трябва да бъде предоставена информация относно необходимостта и целта на събирането на лични данни на потребителя. В случай че такава информация не е предоставена и не ти е предоставена възможност да се обърнеш към администратора/модераторите на съответния сайт или в тях се съдържа информация, която те притеснява, то тогава сигнализирай на горещите линии, като подадеш оплакване. Трябва да знаеш, че всеки администратор/модератор, който поддържа конкретен сайт, е длъжен да даде информация относно това за какво са му необходими твоите лични данни, за какво ще ги ползва, за какъв срок, какво ще се случи с тях, когато те вече няма да са му необходими за тази цел, за която си му ги предоставил (например регистрация), както и на кого и поради какви причини той ще може да ги даде.
11. Не чети и не разглеждай сайтове, които съдържат материали с вредно или незаконно съдържание. Единственото нещо, което те биха могли да ти донесат са вреди, неприятности и проблеми. Няма нищо грешно и лошо в това, че от чисто любопитство, случайно или по съвет от „приятел” в нета си достъпил сайт

с вредно или незаконно съдържание. Не се притеснявай да споделиш това с родител или друг твой близък възрастен човек. Именно той ще ти даде най-добрия съвет как да постъпиш в тази ситуация.

Какво означава „Сайт с вредно съдържание”?
Това са интернет страници, чието съдържание оказва или би могло да доведе да травмиращо психично въздействие или да подтикне техните ползватели към поведение, водещо до психични и/или физически травми.
Какво означава „Сайт с незаконно съдържание”?
Това са интернет страници, на които е публикуван или качен материал, за който в закон е предвидена забрана и се носи съответната отговорност.

12. Използвай на максимум възможностите, които предоставя конкретният сайт за социални контакти за защита на твоя профил и информацията, която си качил на него.
13. Внимавай, когато разговаряш в чат, дискусионни форуми, социални мрежи и т.н. Помни, че хората онлайн често могат да се представят за такива, каквито не са. Важно е да знаеш, че възможността, която предоставя мрежата на теб да останеш анонимен или да се представиш за друг, се предоставя и на всички други участници в нета!
14. Нещата, които правиш в Интернет, не трябва да вредят на други хора или да противоречат на законите. Бъди вежлив и уважавай правата и достойнството на другите участници в интернет.
15. Консултирай се с родителите си, преди да свалиш или инсталираш нова програма на компютъра си. Не прави нищо, което може да увреди компютъра ти или чрез дадено действие от твоя страна да се разкрият данни за теб и семейството ти.
16. Споделяй с родителите си или с друг възрастен твой близък за начините, чрез които се забавляваш, информираш и научаваш нови неща от Интернет.
17. Бъди разумен и изобретателен при избора си на пароли. Помни: Паролите трябва да се променят периодично. Колкото по-дълго време използваш една и съща парола, толкова по-голям е рискът тя да бъде разкрита.
18. Използвай антивирусен софтуер. Обновявай го редовно и не забравяй да сканираш компютъра периодично.
19. В случай, че попаднеш на информация или други неща в Мрежата, които не ти харесват или те плашат по някакъв начин и нямаш възможност да го споделиш с родител или с друг възрастен твой близък, то тогава ти можеш да подадеш сигнал на
адрес: http://web112.net/, http://www.safenet.bg/ или http://www.cybercrime.bg/bg.