Гергана Статева, Ани Василева, Мария Рачева, Ивайло Андреев

ПГХТ "Акад.Н.Д.Зелинский" , гр.Бургас

Урок: Да се изправим срещу кибертормоза - кои фактори интензифицират кибертормоза и насилието онлайн и какво мога да направя да ги намаля?

/Урокът е разработен за преподаване в два учебни часа, необходимо е използването на компютърна зала и интернет достъп/

Основен въпрос

Какво представлява интернет насилието , какви са видовете кибертормоз и как да се предпазя от него?

Обзор на урока

Учениците да се запознаят с видовете кибертормоз. Да се научат да разпознават кога са в опасност от кибертормоз, под каква форма може да се проявява кибертормоза и как трябва да се предпазват и защитават, когато попаднат в ситуаци на кибертормоз. Учениците се насърчават активно самите те да създават събития. По време на обучението те могат винаги да включат своя опит, мисли и възгледи. В допълнение, кооперативните форми на работа и повтарящи се дискусионни елементи в обучението дават възможност за придобиване на социални умения като работа в екип, компетентност за решаване на конфликти и съпричастност.

Цели на урока

Учениците ще могат да:

- Разпознават опасностите в интернет пространството
- Ще се разработят план за поведение, което да ги предпази от кибертормоз
- Ще се научат да проявяват емпатия към жертвите на кибертормоз
- Ще се запознаят с механизмите за противодействие на кибертормоза

Речник

Смишинг, Фишинг, Финансово муле, spear фишинг, E-mail фишинг и измамни връзки

Ход на урока

2-3 мин. - Представяне на темата

Какво разбирате под понятието „Кибертормоз”?

Онлайн тормозът представлява използването на интернет за нанасяне на емоционална вреда върху други хора. Много често той бива използван от деца и тийнейджъри като начин да обидят, отмъстят или просто да се пошегуват с приятелите си. Той има различни форми. Онлайн тормоз може да бъде създаването на фалшив профил във Фейсбук, публикуването на подигравателни снимки или клипове в сайтове като Vbox7 и YouTube, или изпращането на обидни или заплашителни съобщения чрез Viber или

WhatsApp, **п**убликуването на телефонни номера с фалшиви, накърняващи честта и достойнството, обяви.

10 мин. – Допълнително пояснyване на понятието кибертормоз с помоща на рисунка върху дъската./*За целта се рисува облак с изписано понятието "кибертормоз"./*

Учениците създават мисловна карта чрез брейнсторминг.

Подпомагащи въпроси: *Къде и как се случва това?*

10 мин.- Учениците сравняват **тормоза** (лице в лице) и **кибертормоза** като търсят приликите и разликите между двете понятия. Опитват се да изредят видовете кибертормоз, които познават и с които са се сблъсквали.

5-6 мин. – Върху дъската се изброяват видовете кибертормоз /*първо тези видове, които учениците познават, а после и тези, които са непознати за тях. Допълват видовете като ги извеждат от сайта на ГДБОП-МВР* http://www.cybercrime.bg/bg/

10 - 20 мин. – разделени на пет групи те подготвят кратко представяне на пет основни вида кибертормоз. /*Всяка от групите подготвя кратка презентация/*

20 мин.- Представяне на видовете кибертормоз и запознаване на останалите ученици

Всяка група разполага с време да презентира нейните мисли/резултати. Според структурата на класа презентатора трябва да е избран ученик от групата или групата като цяло. След презентацията трябва да осигурите на целия клас пространство за допълнителни предложения, запитвания, дискусии. При това следете часовника, така че всяка група да има достатъчно време, за да представи своето изложение.

/Очакваните отговори и представяне на понятията/

„Смишингът" – при него получавате съобщение или SMS, което ни приканва да отговорим с лични данни или друг вид информация на многократно по-висока тарифа. Да кликнем на линк или звъннем на телефон, за да предоставим поверителна информация или за да заразим устройството си със зловреден код.

„Фишинг" – изпраща се съобщение, което претендира ,че е добронамерено и има за цел да вземе лични данни. Изпращат електронон поща, която претендира, че е от почтенна компания и се опитват да накарат получателя да даде лични или финансови данни.

„Финансови мулета" – престъпниците създават фалшиви обяви за работа и използват жертвите за изпиране на пари

„Spear фишинг"- До определена фирма или организация се изпраща нарочно подготвено електронно съобщение, на което е придаден специфичен вид, че е с доверен източник. Така това съобщение претендира, че е от банкова, международна или друга институция. Като резултат, служителите на атакувана фирма занижават своята бдителност и последват линковете или изпълняват файлове от тези съобщениявърху своите компютърни конфигурации. По този начин престъпниците получавт достъп до заразения компютър на фирмата или до важни потребителски имена и пароли.

„e-mail фишинг и измамни връзки“- фишинг e-mail служат за кражба на лични данни, имена и пароли за достъп, банкови сметки, адреси, електронни пощи и т. н.

Подпомагащи въпроси: *Какви средства и начини за предпазване познавате? Запознаване с целите на специалния сектор „Киберпрестъпност“ към ГДБОП-МВР*

Заключителна част

10 мин. - Обобщаване на резултатите и запознаване на учениците с организацията за борба с кибертормоза чрез използване на сайта на ГДБОП-МВР

Въпросник за обратна връзка

В края на часа раздайте за попълване анонимно следния формуляр за обратна връзка. Погрижете се учениците да обработят въпросника самостоятелно и без „Консултации“ със съучениците си. Съберете въпросници

Питаме за твоето мнение

Темата наистина ми хареса и събуди интереса ми.

Научих много нови неща.

Можех да се включа в разговорите на база досегашния си опит.

Можех да реша добре поставените ми задачи.

Работих интензивно.

Този урок ми беше забавен.

Не ми хареса, беше скучно.