Co-funded by the
Erasmus+ Programme
of the European Union

Сценарий 1
Технологии и ИТ (напр. материали, процеси, производствена организация, ИТ)

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Име на партньор: Foro de Formacion y Ediciones

Този материал е създаден в рамките на проекта BRAIN „BringING STRM into Active AgING“ (ДОГОВОР ЗА БЕЗПЛАТНА СРЕДСТВА 2020-1-PL01-KA204-081805. Този проект е финансиран с подкрепата на Европейската комисия. Тази публикация отразява гледните точки само на автор и Комисията не може да носи отговорност за каквото и да е използване на информацията, съдържаща се в него .

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Име на партньор: Foro de Formacion y Ediciones

Akademia WSEI LUBLIN
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Загрявка

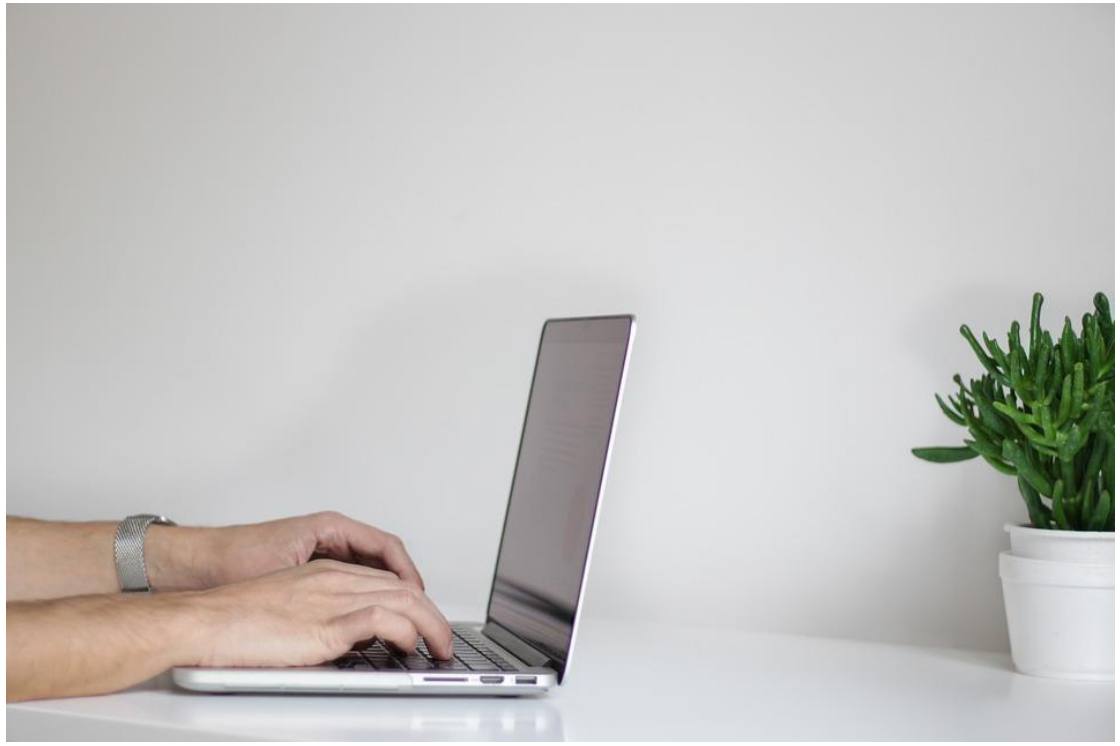
Нека влезем в кръг. След това започнете, като кажете името си и свързана с ИТ дума, която започва със същата буква. Например Adam Application, Bartek Banner, Celine Cookies, Darek Domain и др.…

Тогава следващият човек прави своето, плюс вашето. След това третият човек прави тяхното име, име на втория и първия и дума, свързана с ИТ. След това се движи надолу по линията, така че последният човек трябва да се справи с всички в групата. Могат да се играят различни варианти на това, но е чудесно за запознаване на групата и имената.

Co-funded by the
Erasmus+ Programme
of the European Union

Въведение

Интернет се превърна в определящ фактор за развитието на днешното общество. Той е бил използван като основно средство за взаимодействие между хора и компютри, обмен на информация и насърчаване на бързото предаване на опит и знания, независимо от географското местоположение.



Co-funded by the
Erasmus+ Programme
of the European Union

Въведение

От своето начало през 60-те години на миналия век до наши дни Интернет е основна съставка за технологичното развитие, образованието, комуникациите, медицината, науката, изкуството и практически всички дисциплини и професии. в един глобализиран свят. Въпреки че първоначално е предназначен за военна употреба, ползите от него бяха радикално разширени в практически всяка област.

Co-funded by the
Erasmus+ Programme
of the European Union

Въведение

Търговията е друго пространство, в което интернет успя да окаже положително влияние, както за продавача, така и за купувача. Големите супермаркети и вериги магазини, освен че имат свои пунктове за продажба, са разработили платформи за онлайн продажби, успявайки да намалят някои разходи като търговски персонал и локации, например. Електронната търговия позволява на компаниите да пресичат границите, без да е необходимо да са физически на едно място. Това доведе до ефективност на бизнеса и отвори нови пътища за търговия.

Co-funded by the
Erasmus+ Programme
of the European Union

Въведение

Освен това електронната търговия вече не е изключителна за големите марки. Гъвкавостта на бизнеса позволи на малки и средни компании също да се впуснат в бизнеса, а социалните мрежи дадоха интересен принос за тази динамика.

Co-funded by the
Erasmus+ Programme
of the European Union

Въведение

Следователно интернет днес е глобално средство за комуникация, което ни позволява да взаимодействаме в различни пространства. От комуникация чрез видео разговор или чат с друг човек на хиляди километри, достъп до качествено образование в институти и университети в различни части на света, закупуване на продукти или услуги онлайн, четене на вестници, списания или книги, слушане на музика, гледане на филми , или взаимодействайте в социалните мрежи. Това, за да споменем само някои от многото възможности, които ни предлага.

Co-funded by the
Erasmus+ Programme
of the European Union

Въведение

В нашите ръце е да използваме рационално и обективно инструмент, толкова мощен, колкото бихме искали да бъде.

Начинът, по който интернет се е развил след изобретяването му, е фантастичен и ни позволи да видим, че ще продължи да се развива толкова бързо, че няма да спре да ни учудва.

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите. Флипчарт с фалшиви новини

Материали

телефони/таблети/лаптопи с достъп до интернет, шрайбпроектор, химикалки, маркери, флипчарт, бележки с отметки, листове А4

Упътвания

Водещият записва термина „ФАЛШИВИ НОВИНИ“ в средата на флипчарта. Раздайте 3 листчета на участниците и ги помолете да запишат своите асоциации с термина и да ги залепят на флипчарта. Прочетете написаните асоциации, като ги групирате, ако е възможно. Обсъдете всяка асоциация и я сравнете с определението за фалшиви новини (приложението по-долу).

Приложение

Терминът "фалшиви новини"

Фалшивите новини са „неверни, фалшиви новини, обикновено разпространявани от таблоиди, за да предизвикат сензация или да оклеветят някого (обикновено политик)“. Речникът на Кеймбридж казва, че това е (в превод) „фалшиви истории, които изглеждат като новини, разпространявани в интернет или чрез други медии, обикновено създадени, за да повлияят на политически възгледи или като шега“.

Co-funded by the Erasmus+ Programme of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.
Флипчарт с фалшиви новини

Терминът „фалшиви новини“ е неологизъм и трудно се поставя в дефиниционна рамка. Той обозначава медийни новини, които не са нито верни, нито неверни едновременно и се основават на дезинформация, често включваща верни части. Фалшивите новини обикновено се основават на дезинформация или шега, като често съдържат истински елементи. Фалшивите новини могат да се представят за истинска информация, статии, публикации в социалните медии, мемета и т.н. Те могат да бъдат създадени с различни намерения, от измама до инструменти за пропаганда, за създаване на сензации до шега.
Фалшивите новини са „манипулация на факти, охотно използвана от журналисти, чиято цел при подготовката на публикация е да събудят възможно най-голям интерес към темата, а не нейното съответствие с реалността.
Интернет в момента е най-популярният източник на комуникация. Въпреки това към съдържанието, публикувано в него, трябва да се подхожда с повишено внимание. Проучването на IAB "Дезинформация в мрежата. Анализ на достоверността на информационните канали" показва, че социалните медии са лидер в разпространението на фалшиви новини. На второ място са интернет порталите.

Видове фалшиви новини:
пълна неистина - предоставената информация е измислена, противоречива,
истината е спорна - фактите се представят избирателно или в правилния контекст, което води до подвеждане на реципиента,
манипулиране на цитати - твърдението се поставя в съответния контекст или се премахват изречения или техни фрагменти, което променя смисъла на твърдението и съответно подкрепя конкретната теза.

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите. Видеоклипове с фалшиви новини

Co-funded by the Erasmus+ Programme of the European Union

Материали

телефони/таблети/лаптопи с достъп до интернет, шрайбпроектор, химикалки, маркери, флипчарт, бележки с отметки, листове А4

Упътвания

С помощта на шрайбпроектор водещият показва кратки филми за това какво е фалшива новина и как да я разпознаем.

Как могат да се разпространяват фалшивите новини - Ноа Тавлин (английски, налични са субтитри на други езици)
https://www.youtube.com/watch?v=cSKGa_7XJkg

Как да изберете вашите новини - Деймън Браун (английски, налични субтитри на други езици)
https://www.youtube.com/watch?v=qY-z6HmRgI

Представяне на групата на елементите, благодарение на които можете да разпознаете фалшивите новини, да ги разграничите от истинската информация (приложението по-долу).

Приложение

ИНТЕРПРЕТАЦИЯ НА ИЗВОРНИ МАТЕРИАЛИ:

- обърнете внимание на емоционалния език, бруталните описания
- бъдете наясно със собствените си пристрастия
- задавайте въпроси относно материала (кой е авторът? последователно ли е съобщението? други източници потвърждават ли информацията? и т.н.)

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите. Видеоклипове с фалшиви новини

Co-funded by the Erasmus+ Programme of the European Union

- обърнете внимание дали използваните снимки са поставени в реален контекст
проверете достоверността на уебсайта - дали URL адресът е правилен и води ли до правилния, истински уебсайт
- проверка на датата и актуалността на информацията
- проверете автора - дали той/тя е достоверен, какви са неговите/нейните цели и намерения, дали вече е публикувал други материали онлайн
- проверете дали изображенията не изглеждат странно или не са били манипулирани - това може да се направи например чрез използване на опцията за обратно търсене на изображения, налична в търсачките

ФАЛШИВИ НОВИНИ - ОБЩИ ПРАВИЛА:
В тях преобладават изображения/снимки и кратък текст.
Посланието е силно емоционално натоварено: използва език на омразата, показва насилие, трогателни сцени и образи.
Често се преструва, че е от първа ръка.
Те използват общоизвестни истини и вярвания.
Те често показват полуистина, изопачават фактите по такъв начин, че е невъзможно да се знае къде започва и къде свършва проверената информация. Те се основават на предположението, че една частична истина потвърждава истинността на цялото.
Понякога те описват истински събития, но променят контекста си.
Те почти винаги включват снимки или видеоклипове, за да помогнат за бързото увеличаване на покритието.
Те не съобщават, че предоставената информация може да не е сигурна.
Те избягват нюансите и различните гледни точки.

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Какво можете да ми кажете за поверителността онлайн?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Дефиницията за онлайн поверителност е нивото на защита на поверителността на индивида, докато е свързан с интернет. Покрива количеството налична онлайн сигурност за лични и финансови данни, комуникации и предпочитания. Поверителността в интернет е важна, защото ви дава контрол върху вашата самоличност и лична информация. Без този контрол всеки, който има намерението и средствата, може да манипулира самоличността ви, за да служи на целите си, независимо дали ви продава по-скъпа почивка или краде спестяванията ви.

Co-funded by the
Erasmus+ Programme
of the European Union

Значението на паролите

Паролите са ключът, който отваря вратата за използването на всички наши услуги. Ако паролите ни бъдат разкрити, киберпрестъпниците биха могли да ги използват, за да ги въвеждат и да се представят за нас, да извършват плащания от наше име, да променят или да имат достъп до други видове информация или други хора, наред с други неща, така че е препоръчително да предприемете серия от мерки за нашата защита.

Co-funded by the
Erasmus+ Programme
of the European Union

Значението на паролите

Паролата трябва да е силна, с минимум 8 знака и да се състои от:

-Главен регистър (A, B, C...)

-Числа (1, 2, 3...)

-Малки букви (a, b, c...)

-Специални знаци ($, &, #...)

Важно е да използвате пароли, които не са лесни за отгатване. Например: „123456789“, „qwerty“, „aaaaa“, собствени имена, рождени дни и т.н.

Co-funded by the
Erasmus+ Programme
of the European Union

Значението на паролите

Паролите не трябва да се споделят с никого, паролата трябва да принадлежи изключително на потребителя, който я създава, и да се използва само от потребителя. Споделянето й ще ни направи уязвими и още повече, ако начинът, по който я споделяме, е мрежа за съобщения като (WhatsApp, Telegram, Facebook), тъй като информацията се съхранява на сървърите на тези услуги.

Co-funded by the
Erasmus+ Programme
of the European Union

Значението на паролите

Опитайте се да избягвате използването на една и съща парола за всички услуги на всяка цена, тъй като ако киберпрестъпник се докопа до тази парола, той ще има достъп до всички тях.

Co-funded by the
Erasmus+ Programme
of the European Union

Значението на паролите

Сменяйте паролите периодично, а не постоянни завинаги. Добър начин да запомним кога трябва да променим паролите си е да имаме предвид сезоните на годината. Промяна на паролата за всяка станция, така че винаги да се актуализира на всеки 3 месеца.

Co-funded by the
Erasmus+ Programme
of the European Union

Значението на паролите

Като съвет към целия голям брой пароли, които трябва да се управляват в случай на наличие на една за услуга, има мениджъри на пароли, които улесняват живота, когато става въпрос за запомняне на всички.

Co-funded by the
Erasmus+ Programme
of the European Union

Удостоверяване в 2 стъпки

Понякога наличието на парола не е достатъчно, независимо колко силна може да е тя или след като сте изпълнили всички предишни стъпки.

Киберпрестъпниците могат да се доберат до тях чрез различни техники като „фишинг“ или някои вируси, предназначени за това, които ще видим по-късно.

Co-funded by the
Erasmus+ Programme
of the European Union

Удостоверяване в 2 стъпки

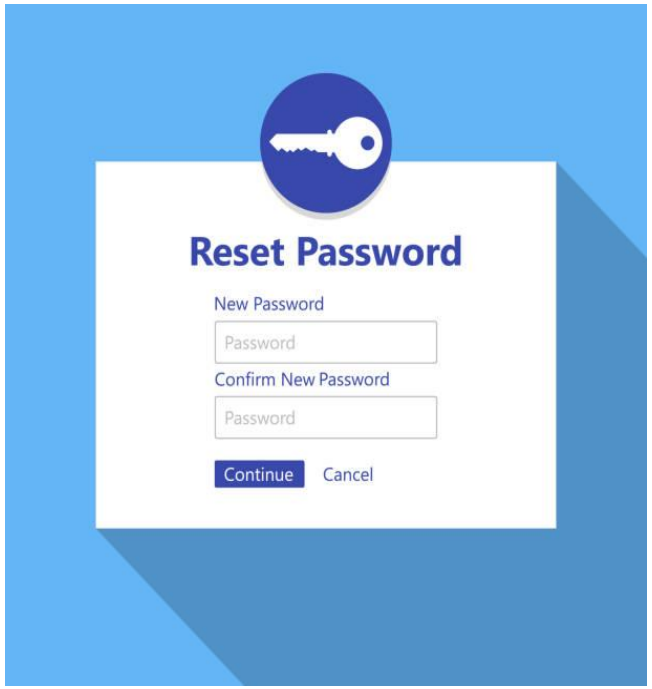
Ето защо много услуги вече предлагат удостоверяване в две стъпки. С този метод ще използваме нашата парола за услугата по нормалния начин и след това ще ни помоли да добавим втори код.

Най-често срещаният начин за получаване на този код е да го получим като SMS на нашия смартфон, въпреки че може да бъде и телефонно обаждане чрез машина или чрез приложение за услуги, което активно променя кодовете на всеки 5 минути.

Co-funded by the
Erasmus+ Programme
of the European Union

Удостоверяване в 2 стъпки

Ясно е, че услугата трябва да бъде предварително конфигурирана, за да свърже нашия смартфон с нея и да получи кодовете. По този начин, дори ако киберпрестъпникът получи вашата парола, той няма да има достъп до услугата, тъй като ще се нуждае от този втори код, за да влезе.



Ако в даден момент откриете, че се опитвате да влезете в акаунта си, защото сте получили двойния код за удостоверяване и това не сте били вие, трябва да помислите за промяна на паролата, тъй като е много вероятно тя вече да не е защитен ключ.

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Какво е шпиониране/подслушване?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Когато сте онлайн, сте шпионирани от редица тракери за различни цели. Проследяващите записват историята на вашето търсене и проследяват всичките ви онлайн дейности чрез различни средства. Това им предоставя ясна представа за това кои сте вие и вашите интереси, което е нарушение на онлайн политиката за поверителност и ви прави обществена собственост. През повечето време това проследяване е само за рекламни цели и позволява на рекламодателите да показват реклами според вашия вкус и интереси. Но понякога тази информация се използва от киберпрестъпници за извършване на неразрешени и незаконни дейности, застрашаващи вашето онлайн съществуване.

Co-funded by the
Erasmus+ Programme
of the European Union

Лични данни

Преди да предоставите вашите лични данни, трябва да анализирате кой ги иска от вас? за какво ти трябва тази информация?

Информацията, която ще трябва да предоставите, например, за да сключите банкова сметка, не е същата като тази при абониране за уебсайт за онлайн пазаруване. В първия случай необходимата информация ще бъде значително обширна, но във втория ще са достатъчни име, фамилия, адрес за доставка, данни за фактуриране и начин на плащане.

Ако някой поиска Вашите лични данни, трябва да се информирате за целта, за какво ще ги използва, както и за тяхното третиране и колко дълго ще съхранява Вашите данни.

Полезно е да знаете как да упражнявате правата си (достъп, коригиране, противопоставяне, ограничаване на лечението и преносимост).

Co-funded by the
Erasmus+ Programme
of the European Union

Фишинг

Фишингът е кражба на самоличност на услуга или компания, за да се опита да измами хората. Например, можете да получите имейл с молба да актуализирате банковите си данни, защото кредитната ви карта е на път да изтече. В този имейл идва връзка за достъп до тази услуга. При отварянето му се появява уеб страница, която е копие на оригинала, потребителят обновява данните на банковата си сметка и тогава е попаднал на измамата.

Co-funded by the
Erasmus+ Programme
of the European Union

Фишинг

Съвети как да не станете жертва

1. Внимавайте с имейли, които изглеждат като банкови организации или добре познати услуги със съобщения от типа:

a. Технически проблеми на предприятието

b. Проблеми със сигурността в потребителския акаунт.

° C. Препоръки за сигурност за избягване на измами.

д. Промени в политиката за сигурност на предприятието

д. Популяризиране на нови продукти

f. Ваучери за отстъпка, награди или подаръци

ж. Предстоящо спиране или деактивиране на услугата.

Co-funded by the
Erasmus+ Programme
of the European Union

Фишинг

2. Бъдете подозрителни, ако в текста има граматически грешки.

3. Ако получавате анонимни съобщения, адресирани до „Уважаеми клиенти“ или „Уведомление за потребителя“, това е индикация, която трябва да ви предупреди.

4. Ако съобщението ви принуди да вземете решение след няколко часа, това е лош знак. Той директно контрастира дали спешността е реална или не с услугата по други канали.

5. Проверете дали текстът на връзката съвпада с адреса, към който сочи.

6. Реномирана услуга ще използва свои собствени домейни за корпоративни имейл адреси. Ако получите съобщението от пощенска кутия от типа @gmail.com или @hotmail.com, това не е добър знак.

Co-funded by the
Erasmus+ Programme
of the European Union

Фишинг

Какво трябва да направите, ако открием случай на фишинг

1. Не отговаряйте на тези имейли при никакви обстоятелства. Ако имате съмнения, попитайте директно фирмата или услугата, която представлява.

2. Не отваряйте връзките, предоставени в съобщението, и не изтегляйте прикачен документ.

3. Изтрийте съобщението и уведомете вашите контакти за измамата.

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Какво знаете за злоупотребата с информация?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Има различни сайтове в интернет, които се нуждаят от вашата лична информация, за да получат достъп до техните услуги. Тези сайтове често съхраняват бисквитки и запазват вашата лична информация, която по-късно я използват за различни цели. През повечето време тази информация не е криптирана и може да бъде достъпна от всеки. Това неправилно боравене с лична информация може да доведе до сериозни последствия. Модерната тенденция на електронното банкиране и порталите за електронен бизнес умножиха рисковете, свързани с поверителността онлайн. Като споделяте вашите банкови данни и важни файлове в интернет, вие проправяте пътища за крадци и се правите уязвими за киберпрестъпници.

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли

Игра: Две истини и една лъжа

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

Игра Две истини и една лъжа. На участниците се дават три твърдения. Две ще са истина, една ще е лъжа. Участниците трябва да идентифицират лъжата.

Приложение

На участниците се дават три твърдения. Две ще са истина, една ще е лъжа. Участниците трябва да идентифицират лъжата. Всички изявления ще бъдат свързани с интернет теми.

Онлайн пазаруване:

1. Кредитната карта е един от най-опасните начини за плащане на стоки онлайн
2. Никога не трябва да въвеждате данните си за плащане на страница, освен ако няма S след HTTP
3. Ако нямате кредитна или дебитна карта, PayPal е добра алтернатива за плащане на стоки онлайн

Зловреден софтуер:

1. Зловреден софтуер е вид компютърен вирус
2. Компютърният червей често експлоатира компютри с остарял софтуер
3. Важна стъпка, за да се предпазите от ransomware, е редовното архивиране

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: Две истини и една лъжа

Фишинг:

1. Ако даден имейл ви адресира като „клиент“, трябва да бъдете особено предпазливи от него
2. Фишинг измама, която знае лични данни, отнасящи се до получателя, се нарича фишинг атака
3. Щракването върху връзка в имейл е допустимо, ако имейлът е от банка, в която имате сметка

Поверителност на социалните медии:

1. Единственото препоръчително ниво на поверителност по подразбиране е САМО приятели и семейство
2. Инсталирането на приложения за социални медии (Facebook, Instagram, Twitter…) може да даде на напълно непознати достъп до определена информация за вас
3. Ако блокирам някого във Facebook или Twitter, този човек няма как да види какво правя с мен или публикувам в моя акаунт

Facebook измама:

1. Добавянето на непознат във Facebook му дава достъп до моя компютър
2. Добавянето на непознат във Facebook може да изложи приятелите ми на риск
3. Добавянето на непознат във Facebook може да доведе до кражба на самоличност

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: Две истини и една лъжа

Co-funded by the Erasmus+ Programme of the European Union

Имейл измами:

1. Имейл измамите с предварителна такса разчитат на измамване на жертвата да изпрати пари с обещанието за много по-голяма възвръщаемост
2. Прикачен файл към имейл, който съдържа документ на Word, все още може да бъде опасен за отваряне
3. Най-добрият курс на действие, ако получа измама с имейл „нигерийски принц“, е да отговоря и да им кажа да спрат да ми изпращат имейли

Ransomware

1. Ако ransomware зарази компютъра ми, надеждна и реномирана антивирусна програма може да го премахне.
2. Антивирусът може да обърне ефектите на ransomware
3. Ransomware е една от най-плодотворните онлайн заплахи за 2017 и 2018 г

След тези примери участниците ще трябва да измислят поне още един. След това те ще се опитат да открият кое твърдение е неправилно.

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: Две истини и една лъжа

Отговори:

1

3

3

1

1

3

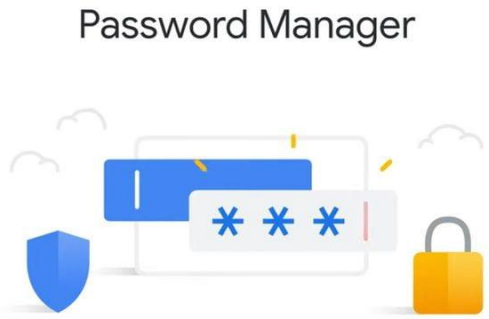
2

Co-funded by the
Erasmus+ Programme
of the European Union

Мениджъри на пароли

Имате безплатна версия на страхотен мениджър на пароли

винаги е по-добре, отколкото да нямаш изобщо.



Co-funded by the
Erasmus+ Programme
of the European Union

Мениджъри на пароли

1Password: страхотна семейна опция ➞ https://cnews.link/get-1password_7/

==========

Минуси на безплатния план:

✓ Проверява за компрометирани пароли

✓ 24/7 поддръжка по имейл

✓ Неограничени потребители за един акаунт

✓ Опция за локално съхранение

1Password

Ограничения на безплатния план:

✗ Няма поддръжка за чат на живо

✗ Няма актуализации на паролата с едно кликване

Co-funded by the
Erasmus+ Programme
of the European Union

Мениджъри на пароли

NordPass: най-универсалният мениджър на пароли ➞ https://cnews.link/get-nordpass_46/

==========

Плюсове на безплатния план:

✓ Криптиране от следващо поколение

✓ Неограничено съхранение на пароли

✓ Многофакторно удостоверяване

✓ Лесни прехвърляния на трезори

✓ Поддръжка на клиенти в чат на живо

Ограничения на безплатния план:

✗ Повечето функции са зад платена стена

✗ Липсват добавки за повече браузъри

Co-funded by the
Erasmus+ Programme
of the European Union

Мениджъри на пароли

Dashlane: сигурно и рационализирано изживяване ➞ https://cnews.link/get-dashlane_39/

==========

Безплатен план:

✓ Споделяне на парола с 5 потребители

✓ Превъзходна репутация

✓ Поддръжка на 2FA

✓ Съхранявайте до 50 пароли

Ограничения на безплатния план:

❌ Максималният брой съхранени пароли е 50

❌ Липсва версия на iOS

❌ Ограничава потребителя до едно устройство

Co-funded by the
Erasmus+ Programme
of the European Union

Мениджъри на пароли

Keeper: изключителен инструмент за управление на пароли ➞ https://cnews.link/get-keeper_10/

==========

Минуси на безплатния план:

✓ Голяма съвместимост

✓ Множество 2FA опции

✓ Приложение за лични съобщения

Ограничения на безплатния план:

✕ Малко опции за експортиране

Co-funded by the
Erasmus+ Programme
of the European Union

Мениджъри на пароли

RoboForm ➞ https://cnews.link/get-roboform_10/

==========

Минуси на безплатния план:

✓ Неограничено съхранение на пароли

✓ Удобно актуализиране на по-слаби пароли

✓ Споделяне на парола чрез имейл

✓ Наблюдение в тъмната мрежа

RoboForm

Ограничения на безплатния план:

✗ Може да бъде по-удобен за потребителя

✗ Чат на живо само за платени потребители

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Можете ли да ми кажете какво е кражба на самоличност и някои от начините, по които се извършва? (фишинг, зловреден софтуер, фарминг, изхвърлени компютри и телефони…)

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Кражба на самоличност и измама със самоличност са термини, използвани за обозначаване на всички видове престъпления, при които някой неправомерно получава и използва личните данни на друго лице по някакъв начин, който включва измама или измама, обикновено за икономическа изгода.

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: С кого говориш?

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

Тази игра трябва да симулира, когато говорите с някого в интернет и всъщност не знаете кой е от другата страна на екрана, дали казва истината или не, или се преструва, че е някой друг за скрита цел.

На всеки участник е определен герой, а другите трябва да разберат кой е той. Но някои от тях няма да отговарят на истината. Тези, които нямат герой по двойки или групи (в зависимост от участниците), трябва да отгатнат чрез въпроси кой е човекът, с когото говорят (този, който има определената роля). Предназначен е за група от 15 души, където 5 имат герои, а 10 по двойки ще се опитат да открият кой е характерът на останалите 5 и дали той/тя е истински или не. Играта ще се играе в две групи от по 15 участници.

Хората с определени герои трябва да отговорят на въпросите, сякаш те са героите. Двойките ще знаят, че е възможно някои от героите да не са тези, за които се представят. Петте двойки ще задават въпроси един на друг за няколко минути и ще се сменят. След като приключи с всички, всяка двойка трябва да каже кой според тях е всеки герой и ако наистина е това, за което се представя.

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: С кого говориш?

Co-funded by the Erasmus+ Programme of the European Union

Персонаж 1:

20 годишно момче. Обича футбола, да излиза с приятелите си и да ходи на концерти.

герой 2:

25 годишно момиче. Играе в отбор по ръгби и харесва планинските спортове. Харесва животни и има куче.

Символ 3: (Фалшив герой)

Отговори като: 18-годишно момиче. Участник по биология. Харесва природата и растенията. Тя е фен на Розалия.

Всъщност той е: мъж на 39 години.

Символ 4: (Фалшив герой)

Отговори като: 23 годишно момче. Харесва рок музика и сърф. Обикновено играе видео игри.

Всъщност той е: 47-годишен мъж.

Знак 5:

27 годишно момче. Той играе падъл тенис. Обича животни и има две котки. Работи като графичен дизайнер.

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: С кого говориш?

Какво се случва?

Тази игра трябва да симулира, когато говорите с някого в интернет и всъщност не знаете кой е от другата страна на екрана, дали казва истината или не, или се преструва, че е някой друг за скрита цел.

На всеки участник е определен герой, а другите трябва да разберат кой е той. Но някои от тях няма да отговарят на истината.

Хората с определени герои трябва да отговорят на въпросите, сякаш те са героите.

Co-funded by the
Erasmus+ Programme
of the European Union

Сценарий 2
Технологии и ИТ (напр. материали, процеси, производствена организация, ИТ)

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Име на партньор: Foro de Formacion y Ediciones

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

Co-funded by the
Erasmus+ Programme
of the European Union

Проблеми с онлайн покупки и парични преводи

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Име на партньор: Foro de Formacion y Ediciones

Co-funded by the
Erasmus+ Programme
of the European Union

Загрявка

Групата образува кръг. Участниците хвърлят топка един на друг. Всеки дава асоциация на предишната дума, изречена от този, от когото получава топката. Дейността се повтаря.

Какво се случва?

Ледоразбивачите са забавни дейности, които помагат на хората да се опознаят. Инструкторите могат да ги използват, за да запознаят участниците със съдържанието и очакванията на курса. Ледоразбивачите също могат да бъдат проектирани да помогнат за затопляне на онлайн учебните пространства и да ориентират участниците към онлайн средата.

Co-funded by the
Erasmus+ Programme
of the European Union

Мобилни плащания

Цифровите портфейли са средство за съхранение на множество физически кредитни или дебитни карти.

Приложение за банкиране, което може да се използва за целите на удостоверяване, ако се изисква при извършване на транзакции или за достъп до банкови услуги. Обикновено всяка банка има собствено приложение.

Co-funded by the
Erasmus+ Programme
of the European Union

Предимства на мобилните плащания

Touch ID под формата на сканиране на пръстови отпечатъци или въвеждане на ПИН ги прави по-сигурни от физическите кредитни или дебитни карти,

Премахване на физически портфейл

Хората не могат да видят каква карта имате (Някои карти се предоставят за клиенти с ниски лимити на кредитен рейтинг. Някои хора се срамуват да я показват на други хора.)

Действайте като по-лесен доставчик на плащания трета страна, когато плащате на уебсайтове за електронна търговия

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Какво представляват бисквитките? За какво са те?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Бисквитките са малки парчета текст, които уебсайтовете, които посещавате, изпращат на вашия браузър. Те позволяват на уебсайтовете да запомнят информация за вашето посещение, което може да улесни повторното им посещение и да ги направи по-полезни за вас. Те са временни файлове, които могат да продължат за по-кратък или по-дълъг период от време. Можем да ги конфигурираме, да използваме инструменти, за да ги блокираме, да ги изтриваме, когато пожелаем... Проблемът може да дойде най-вече когато събират лични данни, без да уведомят потребителя.

Co-funded by the
Erasmus+ Programme
of the European Union

Проблеми с онлайн, покупки с карти и парични преводи.

Безопасно онлайн пазаруване

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

Участниците ще седят в кръга. Обучителят на флипчарта ще пише, задавайки насочващи въпроси на участниците, помагайки им да измислят правила за безопасно пазаруване онлайн (приложението по-долу).

Приложение

- използвайте познат уебсайт
- използвайте инструмента за оценка на безопасността на уебсайта за новите уебсайтове
- потърсете ключалката
- не споделяйте чувствителните си данни с всички
- Използвайте частен Wi-Fi
- Създавайте силни пароли
- Не купувайте с карта на обществени места

Co-funded by the
Erasmus+ Programme
of the European Union

Дигитални портфейли

- **Примери:**
- Apple Pay, Google Pay и Samsung Pay са може би три от най-популярните дигитални портфейли, но има и доста други. Някои други популярни цифрови портфейли включват PayPal и Venmo, като и двата са уникално социални, като ви позволяват лесно да изпращате пари до търговци на дребно и приятели.

Co-funded by the
Erasmus+ Programme
of the European Union

Проблеми с онлайн, покупки с карти и парични преводи.

Опасностите от използването на пари в цифровото пространство

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

Водещият записва термина „Опасности при използването на пари в дигиталното пространство“ в средата на флипчарта. Раздайте на участниците листчета Post-it (различни цветове) и ги помолете да запишат своите асоциации с термина и да ги залепят на флипчарта. Прочетете написаните асоциации, като ги групирате, ако е възможно. Обсъдете всяка асоциация и се опитайте да опознаете онлайн опасностите, свързани с парите (приложението по-долу).

Приложение

Опасностите от използването на пари в цифровото пространство

1. Информацията за вашата карта може да бъде откраднатa (IBAN, CVC, дата на изтичане)

Вашата лична информация може да бъде откраднатa (пълно име, идентификационен код, дата на раждане, телефонен номер, пароли)

Co-funded by the
Erasmus+ Programme
of the European Union

БЕЗОПАСНИ ЛИ СА ДИГИТАЛНИТЕ ПОРТФЕЙЛИ?

Цифровите портфейли всъщност са по-сигурни от физическите карти, тъй като мобилните плащания са силно криптирани и токенизирани, което означава, че никой от вашите действителни номера на карти или сметки не се съхранява в цифровия портфейл.

Дигиталните портфейли отиват още една крачка напред, като добавят и токенизация, която взема тези чувствителни криптирани данни и ги заменя с нечувствителен цифров еквивалент, известен като токен. Тези уникални токени се генерират на случаен принцип всеки път, когато потребител направи плащане и само шлюзът за плащане на търговеца може да съпостави този токен, за да приеме плащането.

Информацията ви не само е по-сигурна благодарение на тази технология, но и чрез проверка на потребителя. Това допълнително ниво на сигурност обикновено се извършва чрез пръстов отпечатък, лицево разпознаване или ПИН.

Co-funded by the
Erasmus+ Programme
of the European Union

Apple и google плащат сходство

И двете системи използват NFC технология

Както Google Pay, така и Apple Pay могат да правят онлайн покупки направо от приложение или уебсайт, като автоматично обработват целия процес на плащане с предварително попълнени настройки по подразбиране и изискват само потвърждение с ПИН или Touch ID за завършване на транзакцията.

И двете са по-сигурни от физическите дебитни и кредитни карти, тъй като системата не разкрива данните за картата на потребителя на доставчика.

Co-funded by the
Erasmus+ Programme
of the European Union

Apple и google pay Разлики

Apple pay позволява удостоверяване с Touch ID или Face ID, но е съвместим само с нови хардуерни джаджи.

Google, от друга страна, избира по-традиционна система за удостоверяване, базирана на ПИН. Това му позволява да работи на по-стар хардуер.

Можете да добавите всяка кредитна или дебитна карта към Google Pay. В apple pay можете да добавяте само кредитни или дебитни карти, с които компанията Apple има контакти с банки, издаващи физически карти.

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Знаете ли какво са облачни данни?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Облачното съхранение е модел на облачно изчисление, който съхранява данни в интернет чрез доставчик на облачно изчисление, който управлява и управлява съхранението на данни като услуга. Доставя се при поискване с капацитет и разходи точно навреме и елиминира закупуването и управлението на вашата собствена инфраструктура за съхранение на данни.

Co-funded by the
Erasmus+ Programme
of the European Union

Google Pay

сигурност на Google? Как работи?

1. Данните за картата на потребителя се предоставят само веднъж, по време на първоначалната настройка на сървърите на Google. (Google съхранява данните за вашата карта на своите сървъри)

2. Google запазва данните за вашата карта на своите сървъри.

3. Виртуалната карта се издава на вашето устройство с криптиране на чувствителни данни.

4. При плащане продавачът никога не вижда вашите реални данни за картата, които са защитени със сървърите на Google.

Co-funded by the
Erasmus+ Programme
of the European Union

Сигурност на Apple?
Как работи?

Pay

- Apple използва система за токенизация.
стъпала;
- Когато данните за вашата карта бъдат предоставени на устройството, то се свързва директно с банката издател. (Apple не съхранява данните за вашата карта)
- Когато картата бъде потвърдена от банката, тя получава специфичен за устройството и картата (свързан) токен, наречен номер на сметката на устройството (DAN), който се съхранява на защитен чип на устройството.
- DAN структурно наподобява номер на кредитна карта и се предава на търговеца, когато се извършва плащане, преди да бъде одобрен от банката.
- Apple pay обяснено подробно:
https://www.youtube.com/watch?v=mt5FEvoEHEk

Co-funded by the
Erasmus+ Programme
of the European Union

Крипто портфейли

Наличието на защитен портфейл за криптовалута функционира много като обикновен портфейл, с изключение на това, че валутите и съдържанието на портфейла могат да бъдат хакнати чрез цифрови средства. Освен това наличието на портфейл може да позволи на потребителите да извършват различни транзакции, като същевременно следят баланса си.

Някои онлайн банки като Revolut, Wirex, Cryptopay и др. позволяват безплатно монети от банкомат в евро/долари до определен лимит.

Revolut

wirex

CRYPTOPAY

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

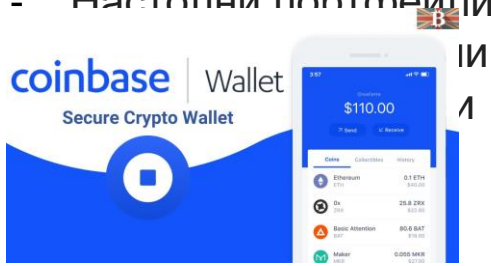
Co-funded by the
Erasmus+ Programme
of the European Union

Видове крипто портфейли

Софтуерни портфейли

Софтуерните портфейли са горещи портфейли, тъй като често са свързани с интернет. Това са портфейли, които работят с определена програма, която позволява лесен достъп. Някои примери за софтуерни портфейли включват:

- Настолни портфейли
- ...ни
- ...и



Хардуерни портфейли

Хардуерните портфейли се различават от софтуерните портфейли в смисъл, че съхраняват личните ключове на потребителя в хардуерно устройство като флаш устройство. Основната им цел е да съхраняват вашите данни офлайн, за да се избегне нахлуване в поверителността. Основната им цел е да съхраняват вашите данни офлайн, ...е избегне нахлуване в по...лността.

Хартиени портфейли

Тези типове портфейли включват конкретен софтуер, който може да се използва за генериране на вашите ключове и отпечатването им. Другите им функции включват прехвърляне на средствата ви на адреса и преместване на активите ви в портфейла на вашия настолен компютър. За да направят последното, потребителите ще трябва ръчно да въведат своите ключове или да ска...ейла.

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Може ли някой да ми каже какво е киберсигурност?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Киберсигурността е практика за защита на системи, мрежи и програми от цифрови атаки. Тези кибератаки обикновено са насочени към достъп, промяна или унищожаване на чувствителна информация; изнудване на пари от потребителите; или прекъсване на нормалните бизнес процеси.

Co-funded by the
Erasmus+ Programme
of the European Union

Предимства на различните видове крипто портфейли

Горещи/онлайн/софт уерни портфейли

- Разходни цели;
- Не желае да плаща за портфейл.

Студени/офлайн/хард уерни портфейли

- Инвестиционни цели;
- Ако съхранявате повече крипто валути, значи

Co-funded by the
Erasmus+ Programme
of the European Union

Проблеми с онлайн, покупки с карти и парични преводи.

Измама при онлайн пазаруване - видеоклипове

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

ЕЛЕМЕНТИ ЗА ДОВЕРДНОСТ НА УЕБСАЙТА

Как да забележите и избегнете измамен уебсайт (на английски):

https://www.youtube.com/watch?v=3oEI0FCnI_Y

Съвети за безопасно пазаруване онлайн (на английски):

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

стъпки:

1. Преди да пуснат видеоклиповете по-горе, участниците са помолени да ги следват и да отбележат не всички елементи на достоверността
2. След като изгледат видеоклиповете, участниците, седнали в кръга, са помолени да напишат елементи за това как да проверят достоверността на уебсайта на флипчарта.
3. Всяко писане се обсъжда незабавно от участника в писането и обучителя (приложението по-долу).

Co-funded by the
Erasmus+ Programme
of the European Union

Проблеми с онлайн, покупки с карти и парични преводи.

Измама при онлайн пазаруване – видеоклипове

Приложение

Как да проверите надеждността на уебсайта:
Платени реклами – някои измамници използват платени реклами от Google, за да се показват в горната част на търсенето с Google.
Положителни фалшиви потребителски отзиви - фалшивите уебсайтове създават положителни отзиви, за да увеличат доверието.
положително фалшиви потребителски отзиви.
Фалшив URL адрес – някои фалшиви уебсайтове използват букви от различна азбука, за да имитират легитимни уебсайтове.
PadLock и HTTPS - показват, че данните, които ще имате в уебсайта, са криптирани. (Трети страни не могат да видят вашите пароли, имейли и др.)
Сертификат - проверете датата на изтичане на сертификата на уебсайта и кой го е издал.
Адрес на компанията. авторски права и контакти - адресът на фирмата не се намира в google maps или е на странно място (гора, пустиня и др.)
Авторски права, оперативен/работен статут - трябва да са актуални.
Фалшиви имейли - по-добре въведете връзки от браузъра си, отколкото от имейлите, защото може да съдържа шпионски данни за събиране на чувствителни данни.

Co-funded by the
Erasmus+ Programme
of the European Union

Дебитна карта

Дебитните карти се **издават от вашата банка и работят като комбинация от банкомат и кредитна карта** . Въпреки това, за разлика от кредитната карта, дебитната карта се свързва директно с вашата банкова сметка, като използва парите, които имате на депозит, за да платите покупката си или да направите цифрово теглене от банкомат.

Co-funded by the
Erasmus+ Programme
of the European Union

Дебитни карти

Професионалисти

- Предотвратете дълга
- Без годишни такси
- Добър за по-малка покупка
- Лесен за получаване

минуси

- Имате ограничени средства
- Имате такси за овърдрафт
- Сложно за артикули с големи цени

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Някой знае ли как се създава силна парола?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Основните ключове за създаване на силна парола са тя да е дълга поне 12 знака, смесвайки главни и малки букви, цифри и символ. Също така е необходимо да използвате различни пароли за всеки сайт и да ги променяте от време на време.

Co-funded by the
Erasmus+ Programme
of the European Union

Кредитни карти

Кредитните карти ви предлагат кредитна линия, която може да се използва **за извършване на покупки, балансови преводи и/или парични аванси** и изисква да върнете сумата на заема в бъдеще. Когато използвате кредитна карта, ще трябва да правите поне минималното плащане всеки месец до датата на падежа на баланса
.

Co-funded by the
Erasmus+ Programme
of the European Union

Кредитни карти

Професионалисти

- Време е да забележите грешки
- Може да изгради кредит
- Предлагайте награди
- Имайте високи лимити

минуси

- Може да загуби не много пари
- Може да навреди на кредита
- Потенциал за преразход

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Какво е VPN?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

VPN означава „виртуална частна мрежа“ — услуга, която ви помага да останете поверителни онлайн. VPN установява защитена, криптирана връзка между вашия компютър и интернет, осигурявайки частен тунел за вашите данни и комуникации, докато използвате обществени мрежи

Co-funded by the
Erasmus+ Programme
of the European Union

Как да сте в безопасност, като използвате своята дебитна или кредитна карта онлайн

Потърсете ключалката: Уверете се, че пазарувате от защитен уебсайт , особено когато е време да въведете номера на картата си. Потърсете иконата на заключен катинар във вашия браузър и обърнете внимание на всички предупреждения за сигурност, които изскачат.

Наблюдавайте акаунта си: Винаги е добра идея да следите парите си и е особено важно, ако споделяте информация за акаунта онлайн. Проверявайте сметките си редовно: поне веднъж месечно, макар че по-често е по-добре. И настройте сигнали в акаунта си, за да знаете кога парите изтичат.

Използвайте сигурни връзки: Мобилните устройства и безплатният Wi-Fi улесняват извършването на нещата. Но никога не знаете колко сигурна е обществената гореща точка . Ако възнамерявате да получите достъп до финансови сметки или да въведете номера на карти, запазете тези задачи, когато сте у дома или на работа, и знайте, че трафикът ви е

Co-funded by the
Erasmus+ Programme
of the European Union

Използвайте познати уебсайтове

- Започнете от доверен сайт. Резултатите от търсенето могат да бъдат фалшифицирани, за да ви подведат, особено когато преминете през първите няколко страници с връзки. Ако познавате сайта, има по-малка вероятност да е измама. Всички знаем, че Amazon.com носи всичко под слънцето; по същия начин, почти всеки голям търговски обект има онлайн магазин, от Target през Best Buy до Home Depot. Пазете се от правописни грешки или сайтове, използващи различен домейн от първо ниво (.net вместо .com, например) – това са най-старите трикове в книгата. Да, продажбите на тези сайтове може да изглеждат примамливи, но това е начинът, по който ви подмамват да се откажете от информацията си.

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Знаете ли как се проследяват потребителите в търсачките? (хронология на търсенията, бисквитки, IP адреси, хронология на кликванията)

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Търсачката може да ви проследява в уебсайтове, ако уебсайтовете, които посещавате, съдържат собствени скриптове за проследяване на търсачката като част от страницата. Това, което търсите, оставя следа от информация за вас. Тази информация разкрива какво ви интересува, какво ви интересува, дори какво мислите за тези неща.

Co-funded by the
Erasmus+ Programme
of the European Union

Потърсете ключалката

- Никога не купувайте нищо онлайн, като използвате кредитната си карта от сайт, който няма инсталирано SSL (слой със защитени сокети) криптиране – най-малкото.
- Ще разберете дали сайтът има SSL, защото URL адресът за сайта ще започва с HTTPS, вместо само HTTP. Ще се появи икона на заключен катинар, обикновено вляво от URL адреса в адресната лента или лентата на състоянието долу; зависи от вашия браузър.
- HTTPS вече е стандартен дори в сайтове, които не са за пазаруване, достатъчно, че Google Chrome маркира всяка страница без допълнителното S като „незащитена“. Така че сайт без него трябва да изпъква още повече.

Co-funded by the
Erasmus+ Programme
of the European Union

Социални медии - сигурно онлайн управление на изображения и информация
Нашата онлайн безопасност и защита на нашата поверителност

Материали

Лаптоп с достъп до интернет за водещия, шрайбпроектор, химикалки, маркери, флипчарт, лепящи бележки, листове хартия А4, топка за тенис.

Упътвания

Водещият разделя участниците на групи от по 4-5 души и ги кара да помислят и напишат на карти отговорите на въпроса: какво можем да направим, за да се погрижим за нашата безопасност онлайн и да защитим поверителността си? След това той моли представители на групите да прочетат отговорите и да ги запишат на дъската/флипчарта. След като запише всички отговори, водещият моли участниците да изберат правилото, което им се струва най-важно. Доброволците казват на другите участници защо са го избрали. Моля, вижте по-долу:

Освен това: Обобщение от инструктора на класа, дискусия за въздействието на социалните медии върху нас, възможностите и рисковете от използването на социалните медии по грешен начин, какво можем да направим нещо, за да увеличим безопасността си.
Съвместно гледане на цялото или части от You Tube видеото "Истината за социалните медии"
https://www.youtube.com/watch?v=DU3655oQexw

Co-funded by the
Erasmus+ Programme
of the European Union

Социални медии - сигурно онлайн управление на изображения и информация
Нашата онлайн безопасност и защита на нашата поверителност

Приложение

- Ако не сте сигурни с кого говорите, не давайте никаква информация за себе си.
- Не разкривайте паролите си на други. Подредете такива, които ще бъдат трудни за отгатване (това не може да бъде вашата рождена дата или име!). Паролата трябва да съдържа не по-малко от 8 знака, включително цифри и главни букви. Използвайте различни пароли за различни услуги.
- Не позволявайте на вашия браузър да запомня пароли за имейли и услуги, които използвате. Излезте, когато сте готови.
- Ако използвате социални мрежи, уверете се, че имате правилните настройки за поверителност. Колкото по-малко информация споделяте с външни лица, толкова по-добре.
- В дискусионни форуми или блогове използвайте псевдоним (псевдоним), а не вашето име. Избягвайте да публикувате информация за себе си онлайн.
- Не използвайте възможността автоматично да се „маркирате“ къде се намирате.
- Обърнете внимание на съобщенията, които се появяват при изтегляне на игри и приложения за мобилни телефони и смартфони. Можете да научите от тях до какви ваши данни иска достъп изтеглената услуга. Внимавайте с какво се съгласявате.
- Предоставете само необходимите данни за създаване на акаунт.
- Вместо Facebook проследяване, използвайте бюлетини и RSS емисии.

Co-funded by the
Erasmus+ Programme
of the European Union

Не споделяйте прекалено много

- Нито един магазин за онлайн пазаруване не се нуждае от вашия социалноосигурителен номер или рождената ви дата, за да прави бизнес.
- Ако обаче мошениците се сдобият с тях и номера на кредитната ви карта, те могат да нанесат много щети. Колкото повече измамници знаят, толкова по-лесно е да откраднат самоличността ви.
- Когато е възможно, по подразбиране се отказвайте от възможно най-малко лични данни. Основните сайтове се нарушават през цялото време.

Co-funded by the
Erasmus+ Programme
of the European Union

Време за въпроси…

Знаете ли за някакви трикове, за да предотвратите проследяването на вашата информация?

Co-funded by the
Erasmus+ Programme
of the European Union

Време за отговор…

Променете настройките, за да блокирате тракери, да използвате инкогнито режим, да използвате VPN, да използвате частни браузъри. Search Encrypt използва криптиране, за да скрие вашата хронология на търсенията от други, които могат да използват вашето устройство, след като търсите.

Co-funded by the
Erasmus+ Programme
of the European Union

Проблеми с онлайн, покупки с карти и парични преводи.

Безопасно използване на кредитни и дебитни карти

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

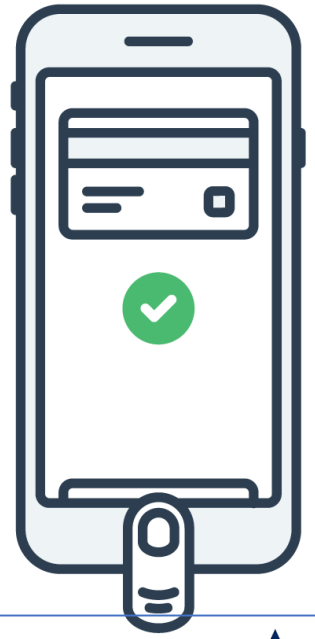
Участниците ще седят в кръга. Обучителят на флипчарта ще пише, задавайки насочващи въпроси на участниците, помагайки им да измислят правила за безопасно използване на кредитни и дебитни карти (приложението по-долу).

Приложение

- Използвайте по-добре мобилно приложение за плащане
- Използвайте функции за безопасност, предоставени от издателя на картата.
- Ако загубите картата си, незабавно уведомете банката
- Не показвайте картата си на публично място.

Co-funded by the
Erasmus+ Programme
of the European Union

Пропуснете картата, използвайте телефона



Плащането за артикули с вашия смартфон е доста стандартно в наши дни във физическите магазини и всъщност е дори по-сигурно от използването на вашата кредитна карта.

Използването на мобилно приложение за плащане като Apple Pay генерира код за удостоверяване за еднократна употреба за покупката, който никой друг не би могъл да открадне и използва.

Освен това избягвате картови скимери – по дяволите, дори не е нужно да носите кредитната си карта със себе си, ако посещавате само места, които приемат плащания по телефона.

Какво значение има това, ако пазарувате онлайн? Много телефонни приложения вече ще приемат плащания чрез Apple Pay и Google Pay. Нуждаете се само от вашия пръстов отпечатък, лице или парола, за да го направите незабавно.

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

Co-funded by the
Erasmus+ Programme
of the European Union

Създавайте силни пароли

- Уверете се, че използвате неразбиваеми пароли. Никога не е по-важно, отколкото когато банкирате и пазарувате онлайн. Нашите стари съвети за създаване на уникална парола могат да бъдат полезни по време на годината, когато пазаруването вероятно означава създаване на нови акаунти в сайтове за електронна търговия.
- Дори перфектната ви парола не е перфектна. По-интелигентният ход: използвайте мениджър на пароли, за да създадете неразбиваеми пароли за вас. Той ще ги следи и въвежда, така че не е нужно да мислите за това.

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: Никога не съм...

Co-funded by the Erasmus+ Programme of the European Union

Материали

Телефони/таблети/лаптопи с интернет достъп, проектор, листове хартия, химикалки, картони

Упътвания

- Всички участници стоят в кръг. Казват се твърдения, започващи с „Никога не съм...“ и участниците, които са направили това твърдение, трябва да направят една крачка напред. След това се връщат по местата си. Тук има няколко примера, но участниците също могат да кажат каквото си искат твърдение.
- Никога не съм пазарувал онлайн
- Никога не съм бил измамен в интернет.
- Никога не съм говорил с някого онлайн, без да го/я познавам
- Никога не съм забравял паролите си
- Никога не съм получавал спам имейл
- Никога не съм бил атакуван от зловреден софтуер
- Никога не съм получавал имейл с искане за цялата си лична информация
- Никога не съм се опитвал да разбера нечия парола
- Никога не съм подозирал, че някой е проникнал в някой от акаунтите ми.
- Никога не съм намирал реклама на телефона си за нещо, което току-що бях търсил.
- Никога не съм подозирал, че съм шпиониран през интернет
- Никога не съм преследвал някого
- Никога не съм страдал от кибертормоз

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: Никога не съм...

- Никога не съм тормозил никого в киберпространството
- Никога не съм влизал в подозрителни уебсайтове
- Никога не съм изтеглял вирус, докато се опитвам да изтегля нещо друго
- Никога не ми се е налагало да променям всичките си пароли
- Никога не ми се е налагало да сменям кредитната си карта, защото данните за нея бяха изтекли
- Никога не съм се представял за някой друг в интернет
- Никога не съм пренебрегвал правилата за запазване на сигурна парола.
- Никога не съм участвал във фалшива томбола в интернет
- Никога не съм губил цялата си работа или нещо важно, защото нямах резервно копие
- Никога не съм щраквал върху банер, който казва, че съм спечелил награда
- Никога не съм сърфирал в Deep web
- Никога не съм споделял лична информация в социалните медии
- Никога не съм споделял неудобни изображения в интернет
- Никога не съм публикувал обидни коментари в интернет
- Никога не съм получавал обидни коментари в интернет
- Никога не съм се опитвал да разбера нечия лична информация
- Никога не съм използвал удостоверяване в две стъпки
- Никога не съм използвал VPN
- Никога не съм се чувствал несигурен в Интернет

Co-funded by the
Erasmus+ Programme
of the European Union

Изтичане на лични данни, създаване на силни пароли, организатори на пароли
Игра: Никога не съм...

Какво се случва?

Игра Never I ever. За интернет темите.
Всички участници стоят в кръг. Казват се твърдения, започващи с „Никога не съм...“ и участниците, които са направили това изявление, трябва да направят една крачка напред. След това се връщат по местата си.
Има някои примери, но те също могат да кажат всяко твърдение, за което се сетят.

Приватизирайте своя Wi-Fi

- Ако пазарувате чрез обществена гореща точка, придържайте се към известни мрежи, дори и да са безплатни, като тези в магазините на Starbucks или Barnes & Noble.
- На всеки от доставчиците в нашия списък на най-бързия безплатен Wi-Fi в цялата страна може да се има доверие, но вероятно трябва да използвате и виртуална частна мрежа (VPN), за да сте в безопасност (ето защо).

Co-funded by the Erasmus+ Programme of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

CRAAP Тест - Презентация

Материали

телефони/таблети/лаптопи с достъп до интернет, шрайбпроектор, химикалки, маркери, флипчарт, бележки с отметки, листове А4

Упътвания

Представяне на инструмента за проверка на информацията (тест CRAAP), за какво се използва и как се използва (приложението по-долу) заедно с Презентацията.

Приложение

Тестът CRAAP е тест за обективната надеждност на източниците на информация в различни научни дисциплини. CRAAP е акроним, който означава валута, уместност, авторитет, точност и цел. Тестът CRAAP е предназначен да помогне на учителите и участниците да определят дали техните източници могат да се вярват. Използвайки теста при оценка на източници, изследователят може да намали вероятността от използване на ненадеждна информация. Тестът CRAAP, разработен от Сара Блейксли и нейния екип от библиотекари в Калифорнийския държавен университет, Чико (CSU Chico), се използва предимно от библиотекари във висше образование. Това е един от многото подходи към критиката на източниците.

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

CRAAP Тест - Презентация

Може да е изкушаващо да използвате всеки източник във вашата статия, който изглежда съгласен с вашата теза, но не забравяйте, че не всяка информация е добра информация, особено в онлайн среда. Разработен от библиотекари в Калифорнийския държавен университет-Чико, тестът CRAAP е полезен контролен списък, който да използвате, когато оценявате онлайн ресурс (или ВСЕКИ ресурс). Тестът предоставя списък с въпроси, които да си зададете, когато решавате дали даден ресурс е надежден и достатъчно надежден, за да бъде използван в научна статия.
Тестът CRAAP е акроним за: валута, релевантност, авторитет, точност и цел. Не е лесно да се определи дали даден източник заслужава доверие и може да се използва като изследователски инструмент. Тестът спестява време и енергия, необходими за оценка на налично съдържание в Интернет.

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

CRAAP Тест - Презентация

Ресурсите трябва да преминат през пет етапа на проверка.
Валута - актуалност на информацията
Времето, когато информацията е публикувана или публикувана, дали информацията е актуализирана или коригирана и дали връзката работи или не.
Релевантност - релевантността на информацията
Проверява дали информацията е свързана с темата, дали ресурсът е уместен и дали може да се използва в учебната работа.
Власт
Изгражда доверие, като предоставя подробности за автора, издателя, преди да се довери на информацията и уебсайта.
точност
Обърнете внимание на точността на съдържанието. Информацията трябва да се основава на доказателства, представени на публиката. Езиковият тон, граматическите и други печатни грешки трябва да бъдат проверени.
Цел на информацията
Определете целите на информацията: информирайте, обучавайте, продавайте, забавлявайте или убеждавайте.

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

Тест CRAAP - Тест

Материали

телефони/таблети/лаптопи с достъп до интернет, шрайбпроектор, химикалки, маркери, флипчарт, бележки с отметки, листове А4

Упътвания

Разделете групата на екипи от около 4 души. Помолете всеки отбор да намери статия по една тема по свой избор. Изберете тема, която отговаря на групата (приложението по-долу). Раздайте отпечатаните крап тестове (приложението по-долу) и раздайте на всеки човек. Помолете участниците да прочетат статията, след което ги накарайте да анализират целия текст в светлината на въпросите, включени в теста. От дясната страна имат място за мисли/заключения/отговори. Въз основа на теста те ще определят колко надеждна е статията. Няма скала за оценяване или брой точки.

Хората работят "онлайн" върху получения материал, което означава, че могат да извършат задълбочен анализ на материала - да научат за цялата статия, да разгледат източника й по-подробно, да проверят използваните данни, да научат нещо за автора и т.н. За тях е важно да проверят, използвайки критериите, дадени в крап теста, дали материалът е достоверен, кои елементи показват достоверността и кои я подкопават. Участниците могат също да запишат своите мисли, което ще улесни дискусията. Помолете всяка група да представи накратко резултатите от своя анализ.

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

Тест CRAAP - Тест

Приложение

Теми за групи:
Климат
Коронавирус
Бежанци
Ваксини
Знаменитости
Спорт
Европейски съюз

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

Тест CRAAP - Тест

		Бележки / отговори
Валута своевременност информация	Кога е публикувана информацията?	
	Актуализирана ли е информацията (ако не е нова)?	
	Случаят, за който преглеждате тази информация, изисква ли по-нови, актуални данни или можете да разчитате на по-стар материал?	
	Работят ли линковете (ако има такива), публикувани в информацията?	
Relevanc материалност на информацията във връзка с вашите нужди	Дали информацията изобщо се отнася до темата, която засягате, или отговаря на въпрос, който е важен за вас?	
	За кого е подготвена информацията? За коя целева група?	
	Информацията на адекватно ниво ли е за вашите нужди? Твърде основен и общ ли е или твърде разширен и подробен?	
	Проверихте ли други източници на информация, преди да решите да използвате само този?	

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

Тест CRAAP - Тест

Власт произход на информацията	**Кой е авторът, издателят, източникът или спонсорът на информацията?**	
	Какви са пълномощията на автора на информацията? С коя организация, образувание, институция е свързан той/тя?	
	Квалифициран ли е авторът да пише по тази тема?	
	Можете ли да намерите информация за контакт, напр. име на издател, имейл адрес и т.н., до информацията?	
	Адресът на уеб сайта, където се е появила информацията, казва ли нещо за автора или подателя (напр. URL адресът завършва на .com, .edu, .gov)?	
точност достоверност, достоверност и точност на информацията	Откъде идва информацията?	
	Предоставената информация подкрепена ли е с доказателства?	
	Информацията била ли е рецензирана или цитирана (отнася се предимно за научни статии)?	
	Можете ли да потвърдите поне част от информацията, дадена в друг източник или използвайки вашите знания?	
	Езикът или произношението на цялата информация показва ли безпристрастност и е лишено от емоционална окраска?	
	Има ли правописни, граматически или стилистични грешки в ситуацията?	

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
HORIZONT X PROCONSULT

Co-funded by the
Erasmus+ Programme
of the European Union

Фалшиви новини - тоест търсене в интернет, проверка на информация, предоставена от медиите.

Тест CRAAP - Тест

Предназначение цел на информацията, причината, поради която е създадена	За какво е създадена информацията? Да образова, информира, забавлява, убеждава?
	Авторът или лицето, финансирало създаването на информацията, дали е ясно каква е целта на информацията?
	Дали информацията е цитат или описание на факти, представя ли мнение или има пропаганден характер?
	Изложената в информацията гледна точка създава ли впечатление за безпристрастност и обективност?
	Виждате ли елементи в информацията, които показват пристрастност, заемане на определена позиция по въпроси, свързани с политика, религия, мироглед или например представяне на гледната точка само на една институция или човек?