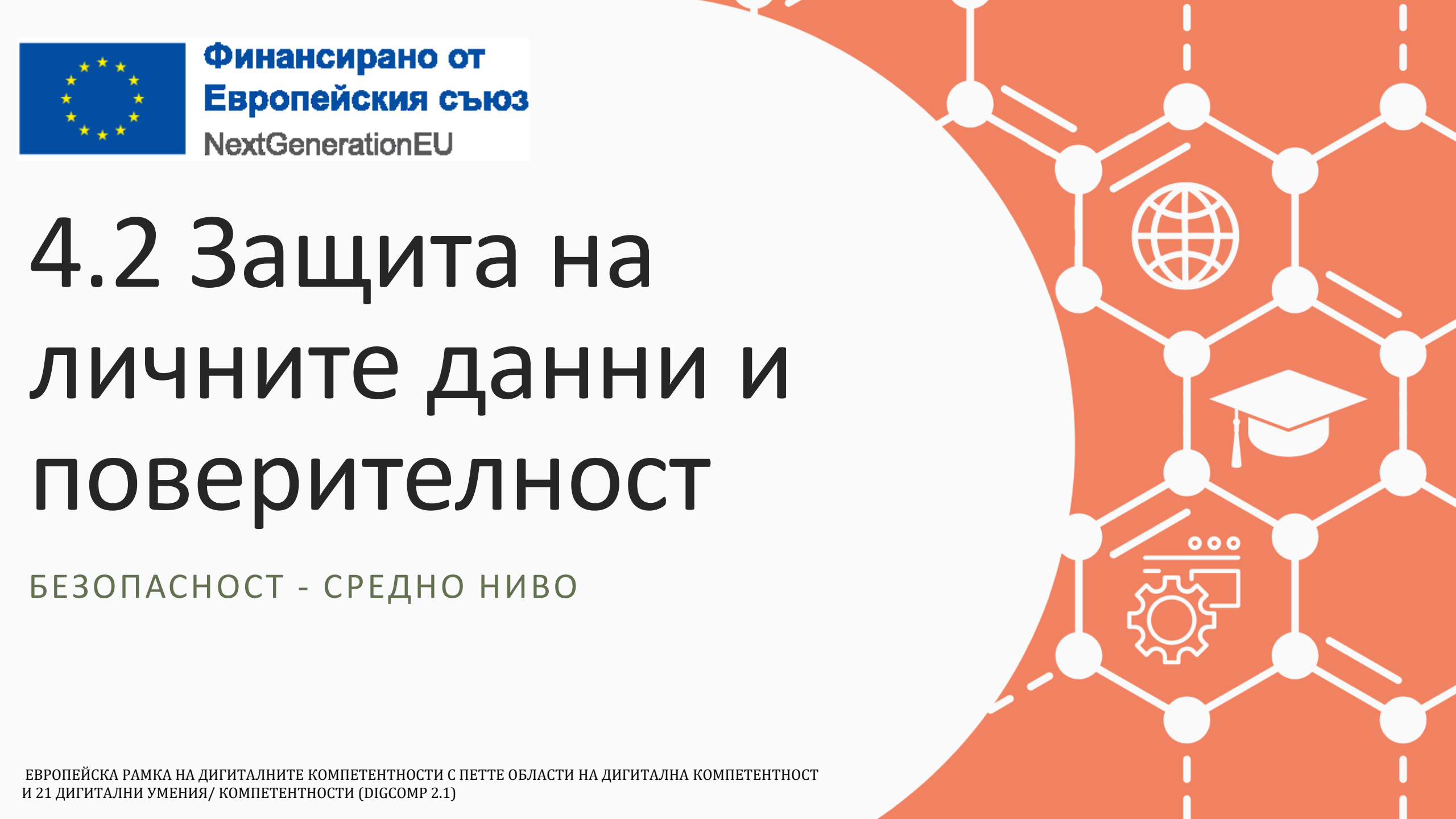
Финансирано от Европейския съюз
NextGenerationEU

4.2 Защита на личните данни и поверителност

БЕЗОПАСНОСТ - СРЕДНО НИВО



ЕВРОПЕЙСКА РАМКА НА ДИГИТАЛНИТЕ КОМПЕТЕНТНОСТИ С ПЕТТЕ ОБЛАСТИ НА ДИГИТАЛНА КОМПЕТЕНТНОСТ И 21 ДИГИТАЛНИ УМЕНИЯ/ КОМПЕТЕНТНОСТИ (DIGCOMP 2.1)

Какво ще научите

- Да познавате начини за защита на личните данни и разпознавате потенциалните рискове и заплахи.
- Да познавате и да може да обясните основните принципи за използване на лични данни при дигитални услуги.
- Да познавате правилата на GDPR и правилата за защита и управление на личните данни.
- Да познавате рутинни подходи за защита на личните данни и неприкосновеност на личния живот в дигитална среда.
- Ще добиете умение да спазвате правилата за защита на личните си данни.
- Ще можете да разпознавате рисково поведение с лични данни.

Защита на личните данни

- Какво представляват личните данни?
  - Информация, която помага на някого да разбере кой си ти (напр. име, рождена дата, телефон, адрес, имейл и др.).
  - Информация, как изглеждаш или звучиш (видео/аудио запис, снимки).
  - Информация за твоите интереси (напр. какво търсиш онлайн) или видове публикации (напр. върху какви най-често щракваш).
- Нива на защита:
  - Лично ниво – защитата на Вашата самоличност, данни и компютърни или мобилни устройства.

    Всеки трябва да знае, че има права и да е запознат с тях, когато споделя личните си данни. *Пример: Правото да поискаш от организацията, която съхранява данните ти, копие от тях, както и да поискаш те да бъдат изтрити.*

Защита на личните данни - 2

- Нива на защита: (продължение)
  - Организационно ниво - отговорност на всеки служител да защитава репутацията, данните и клиентите на организацията.

    Необходимо е да се следва система за сигурност на информацията (съвкупност от правила), която да осигури механизъм за обмен на информацията, за електронни операции и за намаляване на свързаните с информацията рискове на приемливи нива.
  - Правителствено ниво – предвид, че цифрова информация се събира и споделя, нейната защита става още по-важна на правителствено ниво, където националната сигурност, икономическата стабилност и безопасността и благосъстоянието на гражданите са застрашени. Следва се национален протокол по сигурност.

Защита на личните данни - 3

- Тези правила и права се наричат защита на данните и се прилагат, както в реалния свят, така и в онлайн пространството.
- Децата и младите хората имат абсолютно същите права като възрастните, когато става въпрос за техните лични данни, но се нуждаят от своите родители или настойници, които да се грижат за личните им данни вместо тях.

Защита на личните данни - 4

- Основни принципи на информационна сигурност са:
  - Поверителност – да се гарантира, че информацията е достъпна само за онези, които имат разрешение за достъп до нея. Методите за гарантиране на поверителността включват криптиране на данни, проверка на самоличността (напр. потребителско име и парола електронен подпис, биометрични данни или ИД номер) и двуфакторно удостоверяване.
  - Цялостност – да се запази точността и пълнотата на информацията и методите за обработка, с което се гарантира, че данните са защитени от умишлени или случайни промени. Начини за гарантиране на целостта са използването на хеш функция или контролна сума.
  - Наличност – информацията и свързаните с нея активи са достъпни само за оторизираните потребители, когато и където са необходими и следователно физически сигурни. Това може да се постигне чрез поддръжка на оборудването, извършване на навременни хардуерни ремонти, поддръжка на операционни системи и софтуер актуални, създаване и поддръжка на резервни копия.

Защита на личните данни - 5

- Защита на информацията трябва да има и във всяко нейно състояние:
  - Данни, които се използват за извършване на дадена операция, като актуализиране на запис в база данни.
  - Данни в покой - съхранени в паметта или на постоянно устройство за съхранение, като например твърд диск, SSD устройство или USB устройство.
  - Данни, които се трансферират между информационни системи.

Потенциални рискове и заплахи

- Вътрешни заплахи за сигурността – такива, които възникнат от вътре, напр. от настоящ/бивш служител или доверен партньор, при:
  - Неправилно боравене с поверителни данни.
  - Неправилно изпълнение на операциите на вътрешни сървъри или мрежови инфраструктурни устройства.
  - Свързване на заразен външен носител към корпоративната компютърна система, което в последствие да улесни външни атаки.
  - Случайно инсталиране на злонамерен софтуер в мрежата чрез злонамерен имейл или уебсайтове.
- Външни заплахи за сигурността – от външната мрежа:
  - Използват се уязвимости в мрежата или компютърните устройства или
  - Социално инженерство, за да се получи достъп до вътрешната мрежа.

Потенциални рискове и заплахи

- Пробив в сигурността - неоторизиран достъп до данни, приложения, услуги или устройства, разкрива лична информация, която нападателите могат да използват за финансова печалба или други облаги.
- Възможни последици от пробив в сигурността са:
  - Унищожена репутация, вандализъм, кражба, загуба на приходи, повредена интелектуална собственост.
  - Изтичане на чувствителна информация, включително имена на клиенти, имейл адреси, пароли, напомняния за пароли, хешове за удостоверяване, снимки и чат файлове.
  - Получаване на достъп до лични данни на други хора, близки на компрометираните (*Пример. В училище, при изтичане данните на учениците, може да се достигне до записи с данни за родителите*).

Принципи за използване на лични данни

- Категории за класификация на типове лични данни:
  - Доброволно предоставени данни - създават се и изрично се споделят от лица (*Пр. профили в социални мрежи*). Този тип данни може да включва видео файлове, снимки, текст или аудио файлове.
  - Наблюдавани данни – улавят се чрез записване на действията на лицата (*Пр. данни за местоположението при използване на мобилни телефони или заснемане на лицево изображение от обществена камера*).
  - Изведени данни – заключение в следствие на анализ на доброволни или наблюдавани данни – (*Пр. кредитен рейтинг*).

Принципи за използване на лични данни - 2

- Лични данни в персонален план – всяка информация, която може да Ви идентифицира.
- Лични данни в дадена организация:
  - Традиционни:
    - Данни за персонала - материали за кандидатстване, ведомости, договори на служителите; подробности, свързани с покупка и продажба, производствени дейности; данни за основни дейности и операции на организацията.
    - Интелектуални – патенти, търговски марки, продуктови планове, търговски тайни.
    - Финансови - отчети за приходите и разходите, баланси, отчети за паричните потоци.
  - Интернет на нещата (Internet of Things) и големи бази данни (Big Data):
    - Internet of Things (IoT) - голяма мрежа от физически обекти, като сензори, които събират и споделят данни; Big Data – анализ на данните, събирани от IoT сензорите.

Принципи за използване на лични данни - 3

- Мерки за сигурност, използвани за защита на данните:
  - На организационно ниво, както и в личен план, е задължително да се спазват основни и специфични правила по безопасност, за да се гарантира защитеността на данните.
  - Обикновено се изготвят специални документи, който са съвкупност от различни правила и/или регламенти, съобразени с вида на организацията и законодателството на съответната държава, които се наричат политики по сигурност.
  - Всяка организация определя изискванията си по отношение на сигурността и на база на тях се създават конкретни правила, които се описват в нейната политика по сигурност. Препоръчително е да се използват най-съвременните практики за защита.
  - Защита на информационните системи трябва да бъде реализирана още и с решения, както на хардуерно, така и на софтуерно ниво (защитни стени, системи, които непрекъснато наблюдават мрежата в търсене на възможни злонамерени инциденти).
  - Организацията трябва да обучи служителите си как да спазват въведената политика по сигурност, за да са запознати с потенциалните рискове и заплахи и действията за защита, които могат да предприемат, според отговорностите си.

Принципи за използване на лични данни - 4

- От 25 май 2018 г., във всички държави-членки на Европейския съюз се прилагат правила за защита на личните данни, уредени в общия регламент за защита на личните данни (Регламент (ЕС) 2016/679, GDPR).
- Запазват се редица основополагащи принципи и понятия от съществуващата към този момент нормативна уредба, но в същото време се въвеждат по-високи стандарти за защита на данните, разширяват се права на физическите лица и въвеждат нови задължения на администраторите на лични данни.

Правила на GDPR

- Нови моменти в GDPR по отношение на:
  - Права на субекта на данни (физическото лице, за което се отнасят данните).
  - Информацията, която субектът на данни има право да получи от администратора на лични данни при предоставянето на своите лични данни.
  - Случаи, в които субектът на данни има право да поиска от администратора изтриване на неговите лични данни.
  - Ограничаване на обработването на данни от страна на администратора.
  - Право на преносимост на данните (право на прехвърляне на данните към друг администратор).
  - Право на възражение срещу обработването на лични данни за целите на директния маркетинг.
  - По-високо ниво на защита на личните данни на деца.

Правила на GDPR - 2

- Повече разяснения относно ключови въпроси в GDPR за:
  - Изискване на съгласие за обработване на лични данни, което да дава основание за законосъобразно обработване на лични данни.
  - Правото на изтриване (или „правото да бъдеш забравен“) - когато субектът на данни не желае данните му да бъдат обработвани и не съществуват законни основания за тяхното съхранение, да поиска те да бъдат заличени.
  - Профилиране - автоматизирано обработване на лични данни, с цел оценяване на определени лични аспекти, свързани с дадено лице, вкл. за анализиране или прогнозиране на поведението му, изпълнението на професионалните му задължения, икономическото му състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.
  - Въвеждане на длъжностно лице по защита на данните - да осигурява законосъобразното обработване на лични данни в структурата на администратора, да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни.

Правила на GDPR - 3

- Повече разяснения относно ключови въпроси в GDPR за: (продължение)
  - Отчетност - основен инструмент за доказване изпълнението на изискванията на Общия регламент за защита на личните данни. Способността във всеки един момент администраторът на лични данни да удостовери и да докаже, че обработва личните данни законосъобразно, добросъвестно, прозрачно, за конкретни и пропорционални цели, с подходящо ниво на сигурност и защита.
  - Оценка на въздействието - важен инструмент за отчетност, помагащ администраторите не само да спазват изискванията на Общия регламент за защита на личните данни, но и да демонстрират, че са взети подходящи мерки, за да се гарантира спазването на регламента.
  - Защитата на личните данни на етапа на проектирането (privacy by design) и по подразбиране (privacy by default) – нови задължения за администраторите, с които се цели намаляване рисковете за личната неприкосновеност и привеждане на информационните системи в съответствие с изискванията на регламента.
  - Въвеждане на по-строга административно-наказателна отговорност.

Правила за защита и управление на личните данни

- Когато сте онлайн, оставяте дигитална следа, която записва всичко, което правите в различните сайтове и приложения, но и личните Ви данни, които споделяте.

- Стъпки за по-добра защита:
  - Запознайте се с настройките на профила си в социалните мрежи и изберете възможно най-сигурния (препоръчително да е поверителен режим).
  - Преди да публикувате нещо онлайн, помислете добре за кого искате да е видимо, т.к. след това може да бъде трудно да го изтриете.
  - Отнасяйте се с данните на другите така, както се отнасяте със собствените си данни.
  - Преди да се отбележите от някое място (таг-ване, tag), имайте предвид, че това е споделяне на местоположението Ви, което може да Ви изложи на риск. Не давайте разрешение на приложението или сайта да използва местоположението Ви, освен ако не е необходимо.

Правила за защита и управление на личните данни - 2

- Стъпки за по-добра защита: (продължение)
  - Не се оставяйте да бъдете „подведени” – изберете опцията, която е най-сигурна, а не най-лесната за избор! (*Понякога сайтовете и приложенията се опитват да Ви подведат, като искат да предоставите повече лична информация, отколкото им е необходима. Обичайно бутонът, върху който искат да щракнете, е голям, ярък и в средата на екрана, докато другата опция е малка и се пропуска лесно.)* Внимавайте за тези практики!
  - Без да бързате, внимателно прочете условията (*Всеки сайт или приложение трябва да Ви предостави информация за това какво прави с личните Ви данни. Често тази информация е написана на сложен и неразбираем език, затова ако не сте сигурни, попитайте родител или потърсете човек, който да Ви даде компетентен съвет*).
  - Не избирайте просто върху „Приемам всички” (Accept all)

    (*Видите ли съобщение за поверителност или банер за бисквитки, помислете дали искате да ги приемете. Потърсете бутона, който Ви позволява да отхвърлите тези, които можете. В противен случай споделяте повече лична информация, което може да Ви навреди*).

Правила за защита и управление на личните данни - 3

- Стъпки за по-добра защита: (продължение)
  - Знайте стойността на личните си данни (*„Безплатните" услуги не винаги са безплатни. Голяма част от личните данни, споделяни онлайн се използват от приложенията и сайтовете, за да се печелят пари от неща като реклами. Винаги мислете дали си заслужава да споделите твоите лични данни и какво получавате ли срещу тях*).
  - Не забравяйте, че контролът е в Вас (*Когато споделяте личните си данни, Вие имате права върху тях, за които сайтовете и приложенията трябва да се съобразяват. Например Вие можете да поискате от тях достъп и копие от личните Ви данни или да изтрият профилите Ви*).
  - Въвеждайте/предоставяйте точна информация за данните си (*Никога не лъжете за възрастта си или за други данни, когато се регистрирате някъде, както и в социалните мрежи! Това може да доведе до лоши последствия за Вас, тъй като обикновено се съгласявате с определени условия и потвърждавате коректността на данните си*).
  - Изтрийте профила си, когато нямате нужда от него (*Ако вече не използвате някое приложение или сайт, по-добре изтрийте профила си, защото той може да бъде хакнат след време и да се използва от други хора, което впоследствие да Ви навреди*).

Рутинни подходи за защита на личните данни

- Основни стъпки в подходите за защита на личните данни:
  - Създавайте си силни (сложни) пароли

    За да запазите личните си данни, използвайте силни пароли (да съдържат поне 12 знака, от които има малки и големи букви, цифри и специални символи). Старайте се да бъде колкото може по-необичайна и оригинална. Добра практика е да използвате подходяща запомняща се фраза. Не използвайте пароли, които могат да бъдат намерени в речник или са свързани с очевидни неща, които някой друг може да познае (напр. части от Вашето име, името на детето или домашния Ви любимец, рождени дати, любимото Ви телевизионно/Интернет предаване и др.) Добре би било, ако използвате мениджър за пароли.

    (Пример за силна парола: wH-1289757_etV#)
  - Не използвайте една и съща парола за всичко

    Когато използвате една и съща парола за всеки от профилите си, излагате личните си данни на риск. Затова никога не използвайте една и съща парола два пъти. Ако някой разбере Вашата парола, а Вие я използвате на много места, то ще бъдете уязвими.
  - Паролите трябва да се променят периодично – променяйте паролите си през определен период.

Рутинни подходи за защита на личните данни - 2

- Основни стъпки в подходите за защита на личните данни: (продължение)
  - Използвайте многофакторно удостоверяване при влизане от неизвестно устройство или изискване за потвърждение на имейл. Това е добре да се използва особено, когато служители имат достъп до чувствителна информация.
  - Ако нещо Ви изглежда подозрително, не щраквайте върху него, може да е опит за фишинг. (*Получавали ли сте съмнително съобщение от непознат или дори от приятел? Това може да е някаква измама. Не го отваряйте, не щраквайте върху никакви връзки в него и го изтрийте веднага, колкото и да Ви е привлекателно. По-добре да сте в безопасност, отколкото да създадете предпоставки за уязвимост*)

    Най-честите индикатори за фишинг атака са: неофициални или непознати имейл адреси на изпращача; изискване/настояване за изпращане на различен тип лични данни; използваното обръщение обикновено не е лично към Вас, а е общ поздрав или изобщо липсва такъв; посочените хипервръзки, към които Ви насочват, водят към непознати уеб страници или нямат нищо общо с изпращача; езикът и/или стилът на текста е лош или присъстват грешки, което често се дължи на автоматичен превод. Почти винаги присъства и предупреждение за лоши последствия, в случай, че не изпълните посоченото.

Рутинни подходи за защита на личните данни - 3

- Основни стъпки в подходите за защита на личните данни: (продължение)
  - Използвайте само защитени безжични (Wi-Fi) мрежи.

    Незащитените мрежи са много рискови. Злонамерено лице, използващо същата мрежа, може да открадне данните Ви или дори да поеме контрол върху Вашето устройство.
  - Поддържайте устройствата си актуални - Винаги инсталирайте актуализациите възможно най-скоро.

    Когато устройството Ви поиска да инсталирате актуализация, имате възможност да изберете „Напомни ми по-късно” (remind me later), но не отлагайте твърде дълго, защото тези актуализации често съдържат важни защити срещу най-новите вируси и измами.
  - Поддържайте устройствата си сигурни – с инсталирани и включени антивирусен и антишпионски софтуер, както и защитна стена, която е една от най-ефективните защити на потребителски компютър от външни заплахи.

Рутинни подходи за защита на личните данни - 4

- Основни стъпки в подходите за защита на личните данни: (продължение)
  - Постоянно наблюдавайте системите и устройствата си за необичайно поведение, което може да е предизвикано от зловреден софтуер.

    Поддръжката на регистър на действия/събития (логове), където се записват проблеми, грешки или информация за текущи операции е полезна в такива случаи.
  - Регулярното правене на архивни копия е защита от изтриване/унищожаване на съхраняваните данни, както и при хардуерни и софтуерни инциденти.

Въпреки, че можете да спазите всички правила, пълна защита на данните и устройствата не може да се постигне. Киберпрестъпниците постоянно се усъвършенстват. Важно е да сте наясно с често срещаните заплахи и да останете бдителни, както и ако станете жертва, да знаете как да реагирате по възможно най-бързия начин, за да намалите въздействието на злонамерения софтуер.

Въпроси за самопроверка

Въпрос 1. С кое ниво на защита можете да свържете отговорността на всеки служител да защитава репутацията, данните и клиентите на организацията?

A. Лично
B. Социално
C. Организационно
D. Правителствено

Въпрос 2. Кои са основните принципи на информационна сигурност? (Изберете три верни)

A. Цялостност
B. Мащабируемост
C. Наличност
D. Поверителност
E. Достъп

Въпроси за самопроверка

Въпрос 3. Според правилата на GDPR, от субектът на данните се изисква съгласие за обработване на личните му данни?

A. Вярно
B. Невярно

Практическа задача 1. GDPR

Проучете и опишете обобщено, според GDPR:

1. Какви са права на субекта на данни?
2. Какви са категориите лични данни и кои от тях се считат за „чувствителни“?
3. Каква информация най-малко трябва да получите за обработването на личните Ви данни, за да се счита, че имате „информирано съгласие“?

Практическа задача 2. Потенциални рискове и заплахи

Добре известна хотелска верига, е съобщила за масивно нарушение на данните, като личната информация на над три милиона гости е била изложена на хакери. Хотелът открива, че хакери са получили достъп до базата данни с клиенти, използвайки данните за вход на един от служителите му. На този етап хотелът не вярва, че хакерите са успели да получат достъп до пароли за акаунти или финансова информация. Последните гости се насърчават да проверят уеб портала на хотелската верига, за да видят дали са били засегнати от това нарушение.

В този пример какво са взели хакерите? (Изберете правилния отговор)

A. Репутацията на хотелската верига
B. Потребителското име и паролата на всички служители на хотела
C. Информацията за плащане с карта на над три милиона гости
D. Имената, имейл адресите и телефонните номера на над три милиона гости на хотела

В случая е необходимо хотелът да подобри практиките си по сигурност. Какво може да включва това? (опишете/предложете поне три подобрения в сигурността на хотела).

Практическа задача 3. Лични данни и защита

Сигурни настройки на профила в социалните мрежи

1. Прегледайте настройките Ви за защита и вход. Опишете накратко какви методи за защита съществуват за вход и допълнително удостоверяване ?

2. Прегледайте политиките за поверителност на Facebook профила си и проверете следните:

a. Каква информация се вижда за профила Ви и кой може да я вижда.
b. Каква аудитория е зададена по подразбиране да вижда публикациите и историите Ви?
c. Всеки път, когато публикувате актуализация на състояние, снимка или видеоклип, можете ли да избирате кой да ще може да вижда това, независимо от зададената по подразбиране аудитория? Ако да, как става това?
d. Можете ли да докладвате за дадена публикация, че е спам? Ако да, как става това?

Тестови въпроси

Въпрос 1. Коя е една от най-ефективните защити на потребителски компютър от външни заплахи?

A. Включена е защитната стена на потребителския компютър.
B. Пусната е в действие криптировка на пароли.
C. Пусната е системата за обновяване на операционната система.
D. Включена е система за постоянно наблюдение.

Въпрос 2. Кои са често срещани индикатори за фишинг атака? (Изберете всички верни)

A. Неофициални или непознати имейл адреси на изпращача.
B. Заявки за изпращане на лична информация.
C. Общи поздрави или липса на такива.
D. Правописни грешки.
E. Непознати уеб страници и подвеждащи хипервръзки.

Тестови въпроси - 2

Въпрос 3. Кои от следните методи може да се използват за гарантиране на поверителността на информацията? (Изберете три верни отговора)

A. Архивиране
B. Контрол на версиите
C. Криптиране на данни
D. Настройки за разрешение за файлове
E. Двуфакторна автентификация
F. Потребителско име ID и парола

Въпрос 4. Сигурната парола се състои от: (Изберете три верни)

A. Запомняща се фраза
B. Най-малко 6 знака
C. Комбинация от главни букви, малки букви, цифри и символи.
D. Дума, която не може да бъде намерена в речник, не е име на човек, продукт или организация.

Тестови въпроси - 3

Въпрос 5. Кои са трите основни принципи на информационната сигурност? (отворен въпрос)

Въпрос 6. Какъв тип данни са тези, които са заснети с обществена камера? (отворен въпрос)

Въпрос 7: За какво се отнася общият регламент на Европейския съюз, GDPR? (отворен въпрос)

Използвани източници

- Данни, обхванати от правилата на ЕС за защита на данните, включително име, имейл, IP адрес и здравна информация. - https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_bg
- General Data Protection Regulation (GDPR) – Official Legal Text - https://gdpr-info.eu/
- РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА, Официален вестник на Европейския съюз - https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679&from=BG#d1e1518-1-1
- Нови моменти относно правата на физическите лица съгласно Регламент (ЕС) 2016/679 – КЗЛД - https://www.cpdp.bg/?p=element&aid=1178
- Практически въпроси на защитата на личните данни след 25 май 2018 г. – КЗЛД - https://www.cpdp.bg/?p=element&aid=1115
- Набор документи за защитата на личните данни – Вътрешна инструкция за защита на личните данни - https://soplp.files.wordpress.com/2018/05/vatreshna-instrukcia-d183d0bad0b0d0b7d0b0d0bdd0b8d0b5-za-zashtita-na-lichnite-danni.doc
- „Free online tech courses backed by Cisco's expertise and connected to real career paths. Discover your future today.“ - https://skillsforall.com/
- 7 Ways to Recognize a Phishing Email: Email Phishing Examples - https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email