Обработка на информация и комуникация

Разпространение и търсене на информация в онлайн среда
Достоверност, валидност и надеждност на информацията
Заплахи и предизвикателства в интернет-фишинг

Начини за разпространение на информацията:

- традиционните: хартиен носител чрез различни медии, издания, документи и др.

- дигитали и последващ електронен обмен.

Примери за разпространение на дигитална информацията :

- **Електронен обмен на данни EDI (Electronic Data Interchange)** – стандартизиран начин за обмен на делови документи между отделни електронни системи.
- **Уеб-базирани услуги за обработка на въведена информация и предаване на електронни документи, предоставени от различни институции.**
- **RSS (Really Simple Syndication) канали** – удобен начин за бърз и лесен достъп до теми, новини и актуализации на съдържания, без да се налага посещение на конкретен сайт. За целта се използват специални програми, наречени **RSS** четци (уеб-базирани или като приложения за инсталиране), които събират на едно място новините от различни интернет източници (например Google News).
- **Социални мрежи, блогове, чат групи и** др.

1. Достоверност на информацията

Как да преценим дали данните, които намираме в интернет, са верни?

Търсещите машини обикновено извеждат най-вероятните достоверни източници на информация на горни позиции в списъка с резултати.

Получената по електронен път информация е добре да бъде оценена по отношение на достоверност и надеждност, преди да бъде използвана. Обикновено това включва:

- изясняване статуса и актуалността на съобщението;
- установяване точността на информацията – съществуващи грешки и техния характер;
- проверка дали дадената информация е подкрепена с факти;
- съпоставяне на фактите с такива от други източници;
- проучване на компетентността на автора или институцията.

Принципи, при търсене на информация в Интернет:

1. Интернет е публична мрежа - всеки може да публикува всичко. Ако не познавате източника на информация, няма гаранция за нейната достоверност.
2. В повечето случаи информацията, намерена в мрежата, не е проверена за точност.
3. Не всички уеб сайтове са създадени еднакви. Те се различават по качество, цел и пристрастие.
4. Някои уеб сайтове имат спонсори, които плащат за конкретно съдържание, за да рекламират своите продукти или идеи. Информацията там не е безпристрастна.

Принципи, при търсене на информация в Интернет:

5. Някои уеб сайтове изразяват мнения, вместо да дават обосновани аргументи.

6. Някои уеб сайтове са предназначени да бъдат забавни, а не информативни.

7. Някои уеб сайтове се стремят да скандализират и да създадат противоречия, вместо да предоставят надеждна информация.

8. Някои уеб сайтове са стари и информацията, намерена там, не е актуална.

2. Заплахи и предизвикателства в Интернет

Интернет предлага голямо разнообразие от възможни атаки. Въпреки че по-голямата част от тях са малко вероятни трябва да прецените колко опасни могат да бъдат те.

Заплахите могат да се разделят в четири основни категории:

-загуба целостта на данните,

-загуба на конфиденциалност на данните,

-загуба на услуги,

-загуба на контрол.

Компютърните **хакери** са хора, които се опитват да получат достъп до някаква конфиденциална информация.

Докато работиш в Интернет:

Никога не давай лична информация като име, парола, адрес, домашен телефон, училището, в което учиш, месторабота или служебен телефон на родителите си, без тяхно разрешение.

Никога не изпращай свои снимки или снимки на твои близки, без преди това да си обсъдил решението си със своите родители.

Никога не приемай среща с някой, с когото си се запознал в интернет, без съгласието на твоите родители. Ако те одобрят срещата, нека тя да е на публично място и по възможност да е в присъствие на твои близки или приятели.

Никога не отговаряй на съобщения, които са обидни, заплашващи, неприлични или те карат да се чувстваш неудобно. Информирай родителите си за такива съобщения.

Никога не отваряй електронна поща, получена от непознат подател. Тя може да съдържа вирус или друга програма, която да увреди твоя компютър.

Никога не се представяй за някой, който не си. Не скривай годините си и не посещавай сайтове за възрастни.

Винаги внимавай, когато някой ти предлага нещо безплатно или те кани да се включиш в дейност, обещаваща лесна и голяма печалба.

Винаги внимавай, когато разговаряш в чат. Помни, че хората онлайн често се представят за такива, каквито не са.

Винаги бъди вежлив и уважавай правата на другите.

3. Спам (spam)

а) Определение - използване на среда за електронни комуникации за масово изпращане на нежелани съобщения.

Б) Типове:

- **Обикновени непоискани търговски съобщения**, целящи да се реализира продажба на някакъв продукт или услуга.
- **Съобщения с подлъгващо послание**, целящи да се извърши някакво действие, съдържащи например: "пари от интернет", "страхотна гледка", "милионер без наследници" и други.
- **Съобщения със злонамерен характер**, целящи инсталиране на зловреден софтуер, за разпращане на SPAM; за придобиване на лична информация и друго.
- **Съобщения за добиване на чувствителни данни**, като например потребителско име, парола, номер на кредитна карта и др.

В) Съвети за предпазите :

- Отнасяйте се грижливо към своя адрес. Не го публикувайте във форуми, не се регистрирайте с него за съмнителни услуги.
- Не отваряйте и в никакъв случай не отговаряйте на съобщения, които според Вас могат да бъдат определени като Спам. По този начин демонстрирате, че адреса е активен и в резултат ще бъдете затрупани с още реклами.
- Не кликайте върху връзките (линковете), които тези писма съдържат.
- Внимавайте, когато инсталирате безплатен софтуер, защото има приложения, които следят и изпращат Вашия имейл адрес на рекламодатели. За да спре този процес, деинсталирайте подобен софтуер.

АБВ Поща предлага опцията “Защита от Спам”.

Каква е Разликата между спам и спим?

- Спим е спам чрез програми за разговори в реално време.
- Генерира се от компютърни червеи и друг нежелан софтуер. Софтуерът заразява машината и включва хората в списъка с приятели на потребителя, за да им изпраща незабавни съобщения без тяхното знание или съгласие.

СПАМ БОТОВЕ

- Включват се в услуги за съобщения, за да разпространяват порнографски изображения.
- При отговор получавате адрес, който ви кани в частен канал и ви моли да въведете данни за кредитна карта за потвърждение на възрастта.

Ботнет

- Роботизирана мрежа или група компютри, управлявани от хакери.

Филтриране на СПАМ

- Блокирайте адресите, от които получавате спам!
- Използвайте филтри в пощата, за да изпращате ненужните писма в отделна папка.

4. Фишинг

а) Определение

Фишинг атаките са киберпрестъпления, при които потребителите се подвеждат да споделят личните си данни

Напр. Данни за кредитни карти и пароли, и дават на хакерите достъп до устройствата си, *често дори без да подозират*.

По същество това е **инфекция, която атакува компютъра ви подмамвайки ви да го изтеглите.**

Когато обозначаваме видове злонамерен софтуер, като вируси, шпионски софтуер или хардуер, имаме предвид формата, която заразата приема.

Фишингът е изключение от това правило, който описва проблемът, който се е случил, а не *как* се проявява.

В България през 2018 г. се наблюдава висока фишинг активност, която се осъществява с електронни писма, изпратени от името на НАП, различни банки, а в началото на 2019 г. са имитирани и фактури от CEZ.

б)Видове фишинг измами:

- Чрез подвеждащо изпращане на **електронни писма от банката или сървъра**, с който работиш, ти се изисква въвеждане на лични данни - банкови сметки, пароли, потребителско име, достъп до електронна поща. Предоверявайки се ти ставаш жертва и така твоята самоличност вече е достояние на престъпния свят. Мейлите могат да бъдат с обща информация или по-конкретна.

Те имат общ характер и **не съдържат данни за получателя**.

- **Лотарийна измама** - чрез имейл съобщение получаваш информация, че си спечелил голяма сума пари като от теб се искат лични данни.

- **Омографи** - пренареждане на думи с размяна на букви, което в бързината потребителят може да не забележи – например вместо „адрес“ е изписано „ардес“.
- **Маскиране на адреси** - изпращане на имейл линк към фалшиви фишинг сайтове, като понякога се използват данни от легитимни сайтове. Връзката те отвежда към подправен уеб сайт. Не предоставяй лични данни на подозрителни фирми, големите доставчици и компании не биха ти изискали лични данни по имейл.
- **Неотложност като послание в информацията** – фрази от типа спешно, срочно, на момента или „изпратете данни поради срив на системата или спешност“ – не предприемай действие, ако получиш имейл с подобно съдържание и се свържи с източника, за който се представя адресата на имейла.

- **Компрометиране на сметка** - от компроментиран потребителски акаунт изпращане на писма до всички клиенти, фигуриращи в адресната книга. Целта е изготвяне на личен портфейл от данни на жертвите. Тоест може да получиш имейл от реален доставчик, чийто акаунт е бил хакнат с цел измама. Отново не предоставяй данните си онлайн и се свържи с реалния източник / доставчик на услугата.
- **Телефонен фишинг** - Препращане към отдел за поддръжка, на който потребителят-жертва да се обади. Измамникът е от другата страна на линията и приема информацията, която получава от жертвата, използвайки различни мотиви. Измамникът често се представя за служител на финансова организация с атрактивно предложение - намаляване на лихвени проценти или сигнал за грешки в системата, необходимост за възстановяване на личните данни и др.

- SPEAR PHISHING, т.н. **измама харпун** – персонализиран фишинг, в който се проследяват лични потребителски акаунти към институции. Тук прицелването е с точна информация (затова се нарича „харпун“) и измамите могат да бъдат в големи размери. Жертвата и интеракцията й с финансови институции или фирми от бизнеса се наблюдават дългосрочно. Последва фалшив контакт от името на институцията към проследените клиенти с цел пренасочване на плащанията, оформяне на сделки на фалшиви банкови сметки и източване на финансови средства. Увери се, че водиш комуникация с реални представители на действителната институция.

5. Предпазливо поведение в онлайн комуникацията:

- При поискване и предоставяне на лични данни;
- Съобщението към теб е от подозрителен източник, имитиращ реалния, и съдържа насочващ линк, не рискувай да кликнеш;
- Обръщай внимание дали URL адресът е защитен – защитената страница започва с https://..... вместо http://.....;
- Обръщай внимание когато имейлите съдържат грешки – престъпниците често използват онлайн преводачи в опитите си да измамят жертви от различни националности;
- Подхождайте с особено внимание към СПАМ съобщенията – за целта си инсталирай спам филтри;
- Използвай еднократни пароли;
- При попълване на регистрационна форма в официални страници в интернет ползвай виртуална клавиатура.

Спазването на всички тези съвети ти гарантира сигурност на личните данни и средства!

Бъди предпазлив, защото риболовците на данни, т. нар. фишинг измамници, не спят и сърфират денонощно в онлайн пространството в опит да уловят поредните жертви на своите престъпни действия!