

Оценяване на валидността и надеждността на информацията СПАМ



Няколко въпроса

- Когато търсите информация как определяте дали е актуална и достоверна?
- Знаете ли какво е СПАМ?
- Ами СПИМ?
- Вие самите дали сте се сблъскали със спам или спим и какво мислите за него?
- Може ли да се доверите на всяка информация, получена по имейла (например за огромна печалба)?
- Как разпознавате СПАМ-а?
- Как постъпвате, ако получите СПАМ?

Когато търсим информация...

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, а предубедена.
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.

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.
-

Откъде идва понятието СПАМ

Спам всъщност е запазна марка на американската компания за консервирани храни "Хормел Фуудз Корпорейшън". Спам е известна марка консервиран месен продукт, нещо като нашенското Русенско варено. Консерви със "Спам" и до ден днешен се продават в Щатите и дори са част от бойната готовност на Американската армия.

През 1978 г. мениджърът на корпорацията Гари Туърк (Gary Thuerk) се сетил за този евтин начин за реклама и разпратил едно писмо до 393 потребители на ARPANET, вместо да изпрати отделно съобщение за всяко лице.



Откъде идва понятието СПАМ

Понятието Спам обаче придобива смисъла, с който е известно в наши дни, след един скеч на Монти Пайтън от 70-те години, в който се осмива досадният начин, по който тази храна се рекламира. Общо в скеча думата "спам" се споменава повече от 120 пъти.



Къде за първи път се дефинира понятието СПАМ

- Съединените Щати за пръв път дефинират това понятие с точен юридически термин: нарича се UCE (unsolicited commercial email), в превод - непоискани търговски съобщения по електронната поща, и се преследва от Закона.
- Неотдавна Щатският Сенат прие закон, според който **спамът се наказва с до една година затвор и глоба до 500 000 долара!**

Как е в България

В нашия "ЗАКОН ЗА ЕЛЕКТРОННАТА ТЪРГОВИЯ" пише:

"Чл.6. (1) Доставчик на услуги, който изпраща непоискани търговски съобщения по електронната поща без предварително съгласие на получателя, е длъжен да осигури ясното и недвусмислено разпознаване на търговското съобщение като непоискано още с постъпването му при получателя."

Това просто значи, че за деяние, за което в Щатите вкарват в затвора, българският "законодател" просто иска извършителят да "осигури ясното и недвусмислено разпознаване" ... и толкоз!

Видове СПАМ

Спамът се дели на четири основни категории:

1. Изпращане на рекламно съобщение до дори и един интернет потребител, който не е изрично пожелал това.

Видове СПАМ

2. Изпращане до потребители на рекламни съобщения и поща със съдържание, различно от това, за което те са заявили че искат да получават.

Ако например дадете e-mail адреса си за да получавате новини за нови книги, а вместо това получавате и реклами за нови сайтове за бързи кредити, това отново е спам.

Видове СПАМ

3. Изпращане до потребители на рекламни съобщения и поща с честота, различна от обявената.

Ако например се абонирате за месечна информация, а получавате рекламни съобщения ежедневно, спамът отново е налице.

Видове СПАМ

4. Включване на случайни хора в мейлинг листове, като им се предоставя "възможността" да се отпишат.

Това е най-досадния и нагъл тип спам, защото наглед е "законен".

Как да разпознаем СПАМ-а?

- без тема на имейла
- странен имейл на подателя – самият имейл адрес, а не визуализираното име;
- особен текст на писмото – видимо използват автоматичен превод на текста и др.
- понякога спам съобщенията са много добре прикрити зад имената на известни организации като банки, популярни фирми или институции.

YOUR WINNING \$14.850,000.00 MILLIOM

10 март 2018, 02:25

От:



Mrs Helen Diamond

 nazmus@inceptapharma.com

Етикети:



Маркирай ▾



Приложения (0)



Запази всички



Покажи картинките

Функции ▾

Good day

Your email ID won you Fourteen Million Eight Hundred And Fifty Thousand Dollars, So contact Mr James Kangome for more details.

His telephone number (+22969454362) or email him at (diaharold@hotmail.com)

Thanks

Mrs Helen Egobia

от: "Националната агенция за приходите" user123@xyz.com

възстановяване на надвнесения данък

Уважаеми [REDACTED]

Моля, изберете банката си и кликнете върху "продължи", за да пристъпите към плащането на данъка Ви за възстановяване на данъци от: 277 BGN.



Fibank
Първа инвестиционна банка



**UniCredit
Bulbank**

друг

ВАЖНО! - Нови декларации

ОТ: "Националната агенция за приходите" ahoya@goto.tw

дата: 24.10.2020 23:42

1 прикачен файл (~ 6,76 KB)

6,76 KB

deklarac
ia.pdf.exe

Национална агенция за приходите

Уважаеми госпожи/господа,

Националната агенция за приходите Ви напомня, че са в сила нови декларации за 2020г. Необходимо е всички подали реларация по-рано тази година да подадът новия образец на декларация до 30.11.2020 г..

Декларацията може да видите в прикаченият файл.

Известие за анулиране на имейл акаунт

kk [REDACTED]@abv.bg,

обикновено това се изписва
с главна буква

Актуализирахме нашата политика за данни и
потребители за повече безопасност и от вас се изисква
да потвърдите своя потребител сега.

???

Моля, потвърдете имейл акаунта си незабавно, за да
избегнете загуба на вашата пощенска кутия и данни.

???

[Потвърдете потребителя сега](#)

лошо, дори липсващо
графично оформление
на бутона

Благодаря ти,

ABV Подкрепящ отбор

Поддържащ екип,
Екип по поддръжката

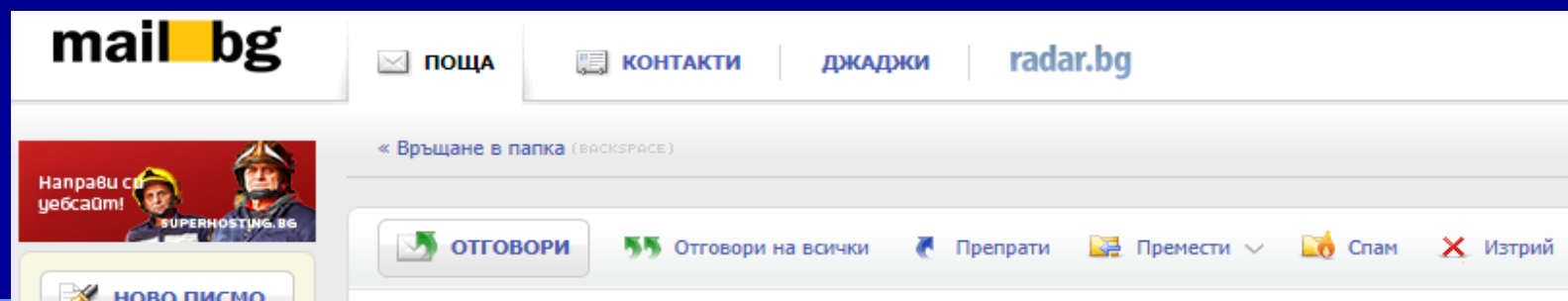
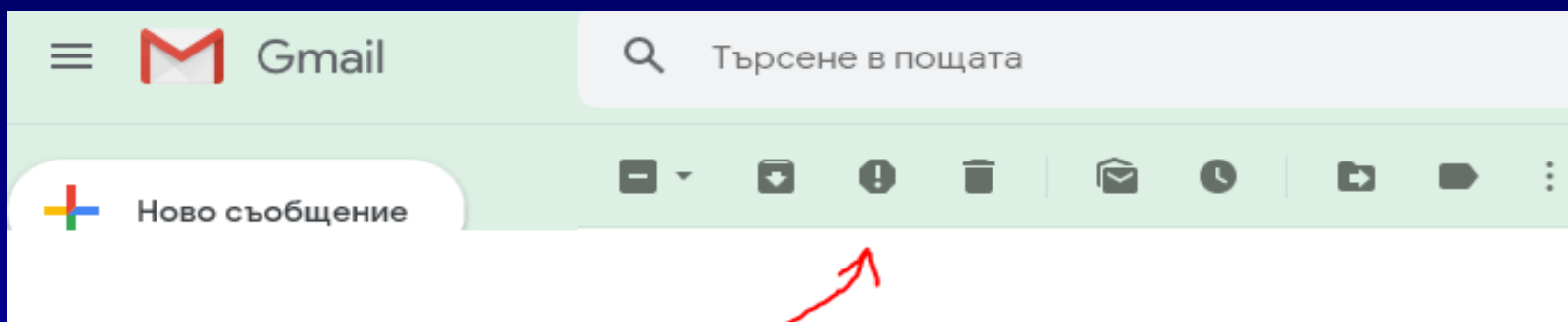
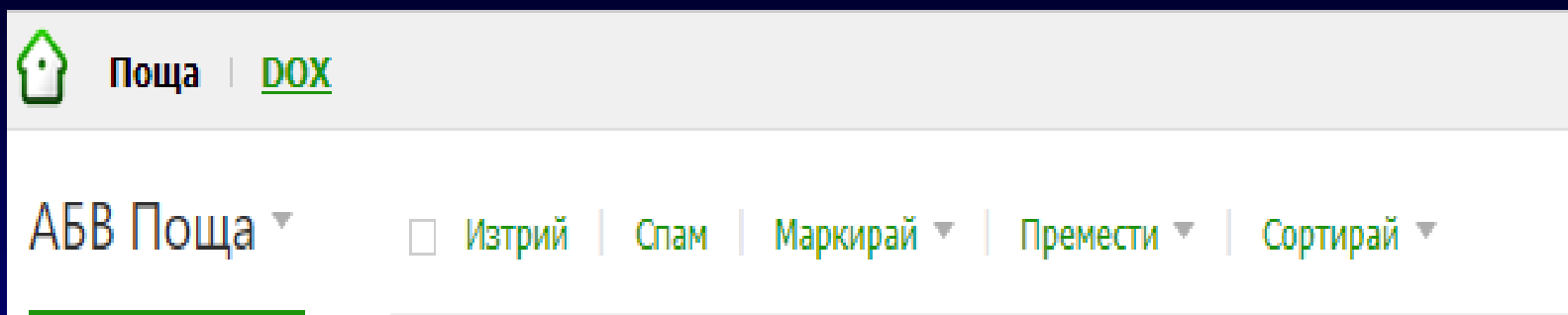
Имейлите ще бъдат изтрети автоматично след 3 дни.
Можете да промените честотата на тези известия във
вашия имейл портал

Липсва "точка"

Разпознават дадено съобщение като СПАМ? Какво направихте?

- изтривате го
- отваряте го
- докладвате го
- отваряте прикачения файл
- щракате на линк, поставен в писмото
- препращате писмото до приятел

Как да се защитим от СПАМ - Филтриране на нежелана поща



Помислете

- Дали всяко изпращане на съобщение до голям брой потребители е спам (например покана от учител до родителите за участие в родителска среща)?
- Какви рискове крие за изпращача разпространяването на информация чрез електронно съобщение до голям брой потребители – напр. може да попадне в папка СПАМ, може да е подсъдно и т.н.

Как да намалим получаването на СПАМ:

1. Направете си официален email-адрес, който не публикувайте в „чист“ вид никъде.
2. Ако ги публикувате, вместо да са изписани по традиционния начин **peter@abv.bg**, да са във вида **peter [at] abv [dot] bg** .
3. Не използвайте официалния си email за регистрации в сайтове, игри, онлайн магазини и т.н.
4. Не го споделяйте в различните месинджъри.

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.

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. Преодоверявайки се ти ставаш жертва и така твоята самоличност вече е достояние на престъпния свят. Мейлите могат да бъдат с обща информация или по-конкретна.
- 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 контактите ѝ 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.

