GENERATION DATA

USING DATA FOR PROFIT

DATASTYRING: SIKKERHED OG PRIVACY

START MED EN HISTORIE

EKSPONERING

I 12. maj 2017 opstod det højeste niveau af ransomware-angreb rettet mod hele verden. Ransomware anvendte udnyttelse kaldet EternalBlue, en sårbarhed, der drives af NSA og frigivet til offentligheden af ShadowBrokers.

Når en computer var inficeret med WannaCry, krypterede den alle hans data. Programmet opstillede en skærm, der krævede en løsesum i form af virtuel Bitcoin for at få tilbage adgang, med løsepenge stigende over tid indtil slutningen af nedtællingen, da alle filerne ville blive ødelagt.

Wannacry påvirkede mere end 200.000 systemer fra virksomheder, offentlige organer og enkeltpersoner i mere end 150 lande. Større organisationer som National Health Services (NHS) [1] i Det Forenede Kongerige og Renault-Nissan måtte stoppe produktionen i nogle områder som et resultat. En række store virksomheder blev også berørt, herunder Telefonica, FedEx, Deutsche Bahn, Santander og KPMG.

Hvorfor var dette angreb så potent?

- For det første den måde, det spredte sig på. Den mest almindelige infektionsrute for konventionel Ransomware var ved at sprede sig via phishing-e-mail og besøge et websted. Ransomware blev distribueret som en mail for at tilskynde brugerne til at klikke på vedhæftede filer i e-mail eller hacke sig ind på en webserver og forklædt som en annonce, så når en bruger besøger webstedet, bliver bruger-pc'en inficeret. Imidlertid havde WannaCry ransomware egenskaber ved en orm, der distribueres autonomt via netværket uden brugerhandling. Hver Windows-computer uden programrettelse var sårbar over for infektionen.

- For det andet ubeskyttede operativsystemer. En af de største bidragydere var, at et stort antal computere ikke havde Microsofts patch installeret eller kørte versioner af Windows, hvor der ikke var nogen patch.

Lektioner

Ledere kunne ikke anerkende, at de for at afskrække og minimere potentialet for cyberangreb er nødt til at sikre, at deres operativsystemer konstant opdateres og patches på tværs af alle netværk.

EKSPONERING

1. DATASIKKERHED

Eksperter advarer om, at WannaCry kun var begyndelsen, og tallene bekræfter denne opfattelse.

Blandt ejere af små virksomheder hersker den uheldige misforståelse, at hackere kun er interesseret i at angribe store virksomheder. Faktum er, at hackere elsker SMV'er. Disse mindre virksomheder har tendens til at fokusere mindre på sikkerhed og har ikke de it-sikkerhedsbudgetter, som store virksomheder har. har ikke midlerne til at betale for sikkerhedsanalytikere eller intern it. [2]

Typer af trusler

[1] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacryransomware-cyber-attack-cio-review.pdf

[2] https://www.telegraph.co.uk/business/cybersecurity-for-small-business/fraud-prevention/

This project has been funded with support from Erasmus+

Et databrud er en hændelse, hvor der er adgang til følsomme eller på anden måde beskyttede oplysninger uden tilladelse. Det kan dræne, hvilke magre ressourcer SMV'er har, og mindske forbrugernes tillid. Kort sagt kan manglende sikkerhed gøre dig konkurs.

2. DATASKYLDIGHED

Hvorfor betyder privatlivets fred?

1. Begræns strøm. Privatliv er en grænse for regeringens magt såvel som magt fra virksomheder i den private sektor. Jo mere nogen kender os, jo mere magt kan de have over os. Personoplysninger bruges til at træffe meget vigtige beslutninger i vores liv. Personlige data kan bruges til at påvirke vores omdømme; og det kan bruges til at påvirke vores beslutninger og forme vores adfærd. Det kan bruges som et værktøj til at udøve kontrol over os. Og i de forkerte hænder kan personlige data bruges til at forårsage os stor skade. [3]

2 Friheder. Privatliv er nøglen til tanke- og ytringsfrihed og hjælper med at beskytte vores evne til at omgås andre mennesker. En nøglekomponent i foreningsfrihed er evnen til at gøre det med privatlivets fred, hvis man vælger. Privatliv er en kritisk komponent i et demokratisk samfund.

3. Rettigheder til en anden chance Mange mennesker er ikke statiske; de ændrer sig og vokser gennem hele deres liv. Der er stor værdi i evnen til at få en ny chance, at være i stand til at bevæge sig ud over en fejl, være i stand til at genopfinde sig selv. Privatliv plejer denne evne. Det giver folk mulighed for at vokse og modnes uden at blive bundet med alle de tåbelige ting, de måske har gjort tidligere

Databeskyttelse er forskellig fra databeskyttelse

- Privatliv er et kompliceret spørgsmål i forbindelse med rettigheder og friheder, der er nedfældet i henhold til loven. Databeskyttelse er forskellig fra databeskyttelse. Beskyttelse handler om at sikre data mod uautoriseret adgang. Databeskyttelse handler om autoriseret adgang - hvem har det, og hvem definerer det. Databeskyttelse er i det væsentlige et teknisk spørgsmål, mens databeskyttelse er en lovlig.
- Teknologi alene kan ikke sikre privatlivets fred for personlige data. De fleste protokoller for beskyttelse af privatlivets fred er stadig sårbare over for autoriserede personer, der muligvis har adgang til dataene. Byrden for disse autoriserede personer handler først og fremmest om fortrolighedsloven, ikke teknologien.

GDPR

- GDPR er en forordning i EU-lovgivningen om databeskyttelse og privatliv for alle individuelle borgere i Den Europæiske Union (EU) og Det Europæiske Økonomiske Samarbejdsområde (EØS). Den vedrører også overførsel af personoplysninger uden for EU og EØS-områderne. [4]
- Det er målet at holde virksomheder ansvarlige for at beskytte de personlige data, der i stigende grad fejes op i nutidens digitale verden
- Det tilkommer de nationale tilsynsmyndigheder - i Storbritannien, Information Commissioner's Office - at håndhæve reglerne for virksomheder inden for deres jurisdiktion.
- Sanktioner: Under GDPR kan tilsynsmyndigheder bøde en virksomhed så meget som 4% af det årlige salg, selvom de fleste bøder hidtil har været langt mindre, typisk mindre end 1 million dollars.

Personoplysninger skal være:

- behandles lovligt, retfærdigt og gennemsigtigt ('lovlighed, retfærdighed og gennemsigtighed')
- indsamlet til specificerede, eksplicitte og legitime formål og ikke viderebehandlet på en måde, der er uforenelig med disse formål ('formålsbegrænsning')
- tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt i forhold til det formål, hvortil de behandles ('dataminimering')

---

3 https://teachprivacy.com/10-reasons-privacy-matters/

4 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

- nøjagtige og, hvor det er nødvendigt, holdes ajour ('nøjagtighed')
- opbevares i en form, der tillader identifikation af registrerede ikke længere end nødvendigt for de formål, hvortil de personlige data behandles ('opbevaringsbegrænsning') behandles på en måde, der sikrer passende sikkerhed af
- personoplysningerne, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod utilsigtet tab, ødelæggelse eller beskadigelse ved hjælp af passende tekniske eller organisatoriske foranstaltninger ('integritet og fortrolighed').

British Airways casestudie

- En halv million passageroptegnelser blev åbnet i et cyberangreb mellem 21 St. Aug og 5 th Sept 2018. Virksomheden løste overtrædelsen af sin hjemmeside og app den 6. th Sept og politiet blev underrettet.

- Informationskommissærens kontor (ICO) oplyste, at en række oplysninger blev kompromitteret af dårlige sikkerhedsordninger, herunder login-, betalingskort- og rejseoplysninger samt navn og adresseoplysninger.

- Flyselskabet bliver nødt til at betale £ 183,39 millioner ($ 230 millioner) til ICO for ikke at beskytte sine kunders data, den største sanktion iværksat af nationale reguleringsmyndigheder i hele EU siden vedtagelsen af GDPR. [5]

3. DATAETIK

Datakraften er så stor og kan have en så stor indflydelse på vores liv, at vi ikke skal forestille os data som Is og Os, men som en digital sjæl. Begrebet en 'digital sjæl' blev beskrevet som den elektroniske repræsentation af dig selv. At skabe en model for ejerskab og kontrol af denne idé er den store udfordring for virksomheder, der har data, såvel som enkeltpersoner og regulatorer

Lessigs patetiske prik

Den patetiske prikteori eller New Chicago School-teorien blev introduceret af Lawrence Lessig i en artikel fra 1998 og populariseret i sin bog fra 1999, *Kode og andre love i cyberspace*. Det er en socioøkonomisk teori om regulering. [6] Den diskuterer, hvordan individers liv (de patetiske prikker i spørgsmål) reguleres af fire kræfter: loven, sociale normer, markedet og arkitekturen (teknisk infrastruktur).

Teorien fremhæver, hvordan computerkode kun er en af de lovgivningsmæssige modaliteter, der kan ændre adfærd, og det er derfor vigtigt at forstå andre mekanismer som lov, normer og etik for bygningsteknologier, der ikke resulterer i uønsket adfærd.

Dataetik handler om at gå ud over lovgivningen og forstå, hvordan markeder, normer og kode interagerer for at sikre, at vi er etiske i vores brug af individets data. Vi skal gå ud over overholdelse og bruge data på den bedst mulige måde for alle involverede.

Tre store temaer

Samtykke. Samtykke er, hvad mange mennesker diskuterer, når de tænker på teknologisk etik.
I henhold til GDPR er kravene til samtykke blevet styrket for at kræve en positiv og utvetydig handling for at 'tilmelde sig'. Det er ikke længere en engangsbeslutning, men et løbende spørgsmål at være omhyggelig

---

5 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announcesintention-to-fine-british-airways/

6 https://en.wikipedia.org/wiki/Pathetic_dot_theory

overvåges. Enkeltpersoner kan når som helst trække deres samtykke tilbage uden straf. Mekanismerne til at trække samtykke tilbage bør være lige så lette som dem til at give samtykke. Enkeltpersoner skal have et ægte valg om, hvorvidt de giver deres samtykke. Hvis de ikke har et valg, anses samtykket ikke for at være givet frit og vil ikke være gyldigt.

Datadeling . Stærk etisk og risikoreducerende praksis udelukker deling af data uden samtykke fra de mennesker, der afslører dem. De udelukker også deling af data med parter, som der ikke er givet adgang til. Men effektiv anvendelse af data kræver, at de deles - og især i den digitale forretnings æra med en voksende platformøkonomi. Flere og flere organisationer samarbejder om at skabe nye tilbud og endda nye industrier. Disse samarbejder nødvendiggør udbredt og konstant datadeling, hvilket medfører nye og vanskelige forudsigelige risici. Disse risici forstærkes af det faktum, at når datasæt når en stor nok størrelse, er anonymitet en myte. [6] Og når yderligere datasæt sammenlægges, kan enkeltpersoner identificeres med relativ lethed. [7], [8] Løsning af problemer og skader forbundet med deling data, [7])

Algoritmisk ansvarlighed og bias. Måder, hvorpå klassificeringsalgoritmer kan tilpasses eller evalueres for at mindske potentielle bias eller gennemsigtighedsproblemer. I årevis har snesevis af rapporter fra organisationer som ProPublica eksponeret omfanget af algoritmisk diskrimination i vurdering af kriminel risiko , forudsigelig politiarbejde , kreditudlån , ansættelse , og mere. Bias kan være et menneskeligt problem, men *forstærkning* af bias er et teknisk problem - et matematisk forklarbart og kontrollerbart biprodukt af den måde, modellerne trænes på.

Bare fordi en algoritme er retfærdig, betyder det ikke, at den bruges retfærdigt. Praktikere bør handle ved nøje at gennemgå algoritmiske tilgange til afbødning af bias. Det er vores ansvar at kritisk forhøre, hvem der drager fordel af disse teknologier, hvis omkostninger er, og at tale om, hvordan vores modeller skal eller ikke skal bruges.

Eksempler på algoritmisk bias

Ansigtsgenkendelsessoftware bruges i stigende grad til retshåndhævelse - og er det en anden potentiel kilde til både race og kønsforstyrrelse . I februar i år fandt Joy Buolamwini ved Massachusetts Institute of Technology, at tre af de nyeste kønsgenkendelses-AI'er fra IBM Microsoft og det kinesiske firma Megvii korrekt kunne identificere en persons køn fra et fotografi 99 procent af tiden - men kun for hvide mænd. For mørkhudede kvinder nøjagtighed faldt til kun 35 procent . Det øger risikoen for falsk identifikation af kvinder og mindretal. Igen er det sandsynligvis ned til de data, som algoritmerne trænes på: hvis det indeholder langt flere hvide mænd end sorte kvinder, vil det være bedre at identificere hvide mænd. IBM meddelte hurtigt, at det havde omskoleret sit system til et nyt datasæt, og Microsoft sagde, at det har taget skridt til at forbedre nøjagtigheden.

Kilde: Ny videnskabsmand: https://www.newscientist.com/article/2166207-discriminating-algorithms-5times-ai-showed-prejudice/#ixzz5vqEWBlh2

4. INFORMATIONSSTYRING

Dataovertrædelser er alvorlige, og kunderne kræver stadig bedre opmærksomhed på dataetik, så vi er nødt til at tage datastyring alvorligt. Virksomheder har brug for en nødplan, men forebyggelse er bedre end helbredelse.

Der er ingen løsning, der passer til alle.

---

7 https://www.accenture.com/_acnmedia/pdf-22/accenture-data-ethics-pov-web.pdf

Definition: "... specifikation af beslutningsrettigheder og en ramme om ansvarlighed for at tilskynde til ønskelig adfærd i værdiansættelse, oprettelse, opbevaring, brug, arkivering og sletning af information." (Logan, 2010). For ord indeholder det et sæt regler og vejledning til, hvordan data eller information håndteres i en organisation. (Citeret i Rising, Kristensen, Tjerrild-Hansen, 2014 [8])

Mål

1. maksimere værdien af information for organisationen ved at sikre, at informationen er pålidelig, sikker og tilgængelig for beslutningstagning
2. beskytte information, så dens værdi for organisationen ikke mindskes gennem teknologi eller menneskelige fejl, tab af rettidig adgang, upassende brug eller misadventure.

Hvorfor er det informationsstyring og ikke datastyring?

”Kort sagt, data refererer til rå, uorganiserede fakta. Tænk på data som bundter af bulkindgange samlet og gemt uden kontekst. Når kontekst er blevet tilskrevet dataene ved at strenge to eller flere stykker sammen på en meningsfuld måde, bliver det information. ” Lebanthal

4 Risikovurdering

En risikovurdering hjælper dig med at forstå de områder, du har brug for at beskytte, dem, hvor du kan være mest sårbare og potentielle worst-case scenarier. Start med at kontrollere de data og oplysninger, du har, som er mest værdifulde. Se derefter på, hvordan du gemmer disse data, hvem der har adgang til dem, og hvordan de er beskyttet af teknologi og processer, for at forstå, hvor du kan være mest udsat. Hvis du ikke er sikker på at udføre en risikovurdering, kan du overveje at ansætte en ekspert til at gøre dette for dig.

En effektiv reaktionsplan bør omfatte følgende elementer:

- Dit juridiske svar: Du er nødt til at redegøre for, hvordan du håndterer de juridiske aspekter af overtrædelsen, for eksempel at informere Informationskommissærens kontor (ICO) om problemet og forsvare din virksomhed mod påstande om uagtsomhed.
- Håndtering af medieforespørgsler: Din virksomhed kan være i fokus for medieopmærksomhed efter et brud, så vær klar til at håndtere al ekstern kommunikation om, hvad der skete, og hvordan du håndterer det. Du har sandsynligvis brug for professionel PR-ekspertise for at gøre dette effektivt. Find ud af, hvad der skete: Du bliver også nødt til at have it-kriminaltekniske eksperter ved
- hånden for at finde ud af, hvad der forårsagede overtrædelsen med henblik på at rette op på problemet hurtigt og sikre, at det ikke sker igen.

- At informere kunder: Afhængigt af din kundebase og omfanget af overtrædelsen kan du have mange ubehagelige telefonopkald at foretage! Du bliver nødt til at være klar med en måde at håndtere denne kommunikation effektivt på.

BEMÆRK TIL

Cyberforsikring

Hvis du står over for konsekvenser af et databrud , din sidste forsvarslinje er vandtæt og specialis t cyberforsikring . Dækker dig for overtrædelse af databeskyttelseslove (hvor det er forsikringspligtigt ved lov) og dit ansvar for håndtering af data, kan det også dække afpresning, omkostninger til systemretning plus PR-udgifter og økonomisk tab på grund af systemets nedetid.

Nogle vigtige aspekter at passe på inkluderer:

- Informationskommissærens kontor (ICO) kan give bøder på op til £ 500.000 for overtrædelse af databeskyttelsesloven. Den digitale risiko cyberforsikring dækker udgifter til underretning,

8 https://web.stanford.edu/class/msande238/projects/2014/GainIT.pdf

advokatgebyrer, der forsvarer lovgivningsmæssige handlinger, og i nogle tilfælde selve sanktionen (hvor dette lovligt kan forsikres).

- Dæk til dine out-of-pocket udgifter, som kan omfatte systemreparationsomkostninger, mistede indtægter, mens systemet er nede eller endda løsepenge til hackere.
- Dækning til dit websted, blogs og sociale medier, overtrædelse af ophavsret eller varemærke eller ærekrænkelse osv.

Casestudier

Facebook-socialsikringsstudie

GENERATION DATA

USING DATA FOR PROFIT

CYBERNET SIKKERHEDSCENTER UNDER FORSVARSMINISTERIET

FACEBOOK SOCIAL SIKKERHED

Hvorfor kan din personlige konto være nyttig?

• For personlige oplysninger om dig:

o Kontakter o billeder; o andre personlige oplysninger (når du gik, hvor du gik, hvor du bor, betalt, arbejde, hobbyer, hobbyer osv.);

• For information om de mennesker, du kommunikerer med;

• Falske sidebedømmelser, kommentarer osv .;

• For Facebook-grupper og sider administreret af din konto.

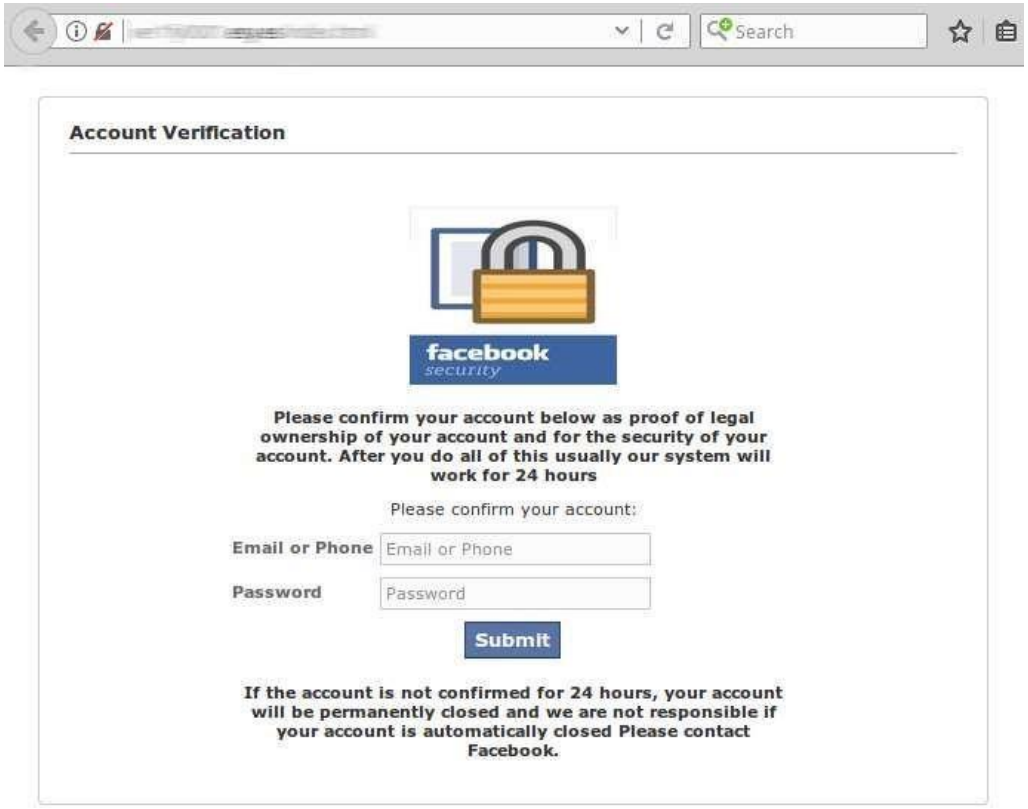
Der lægges særlig vægt på Facebook-grupper, sider og enkeltpersoner - især dem, der har et betydeligt antal tilhængere. Stjålne Facebook-sider og konti sælges ondsindet til tredjeparter, udnyttes til reklame og andre formål.

Hvordan kapres Facebook-konti?

• Mest stjålne adgangskodebeskyttede konti;

• Loginoplysninger kommer fra andre kilder (e-mail, andre online-konti); • Loginoplysninger indsamles på offentlige enheder og offentligt tilgængelige gratis trådløse netværk (gratis wifi);

• Login stjålet gennem social engineering (ved at sende falske e-mails med links til phishing på Facebook)



Figur 1. Et eksempel på social engineering er forfalskning af sider

Ansvar for uautoriseret login til din Facebook-konto.

Ansvar for sådanne aktiviteter er beskrevet i artikel 198 1, stk. 1, og 198 2, stk. 1, i straffeloven for Republikken Litauen.

Artikel 198 1. Ulovlig adgang til informationssystemet

Den, der ulovligt har fået adgang til informationssystemet eller en del af det i strid med informationssystemets sikkerhedsforanstaltninger, der kan straffes med offentlige arbejder eller bøder, eller anholdelse eller fængsel i op til to år.

Artikel 198 2. Uautoriseret bortskaffelse af enheder, software, adgangskoder, koder og andre data

Enhver, der til kriminelle formål eller på anden måde har produceret, transporteret, importeret, solgt, stillet til rådighed eller på anden måde distribueret, erhvervet eller besat udstyr eller software, der er direkte beregnet til eller tilpasset til at begå forbrydelser, samt adgangskoder, koder eller andre lignende data til logning videre til et informationssystem eller en del deraf, der kan straffes med offentlige arbejder eller med bøder, eller ved anholdelse eller fængsel i op til tre år.

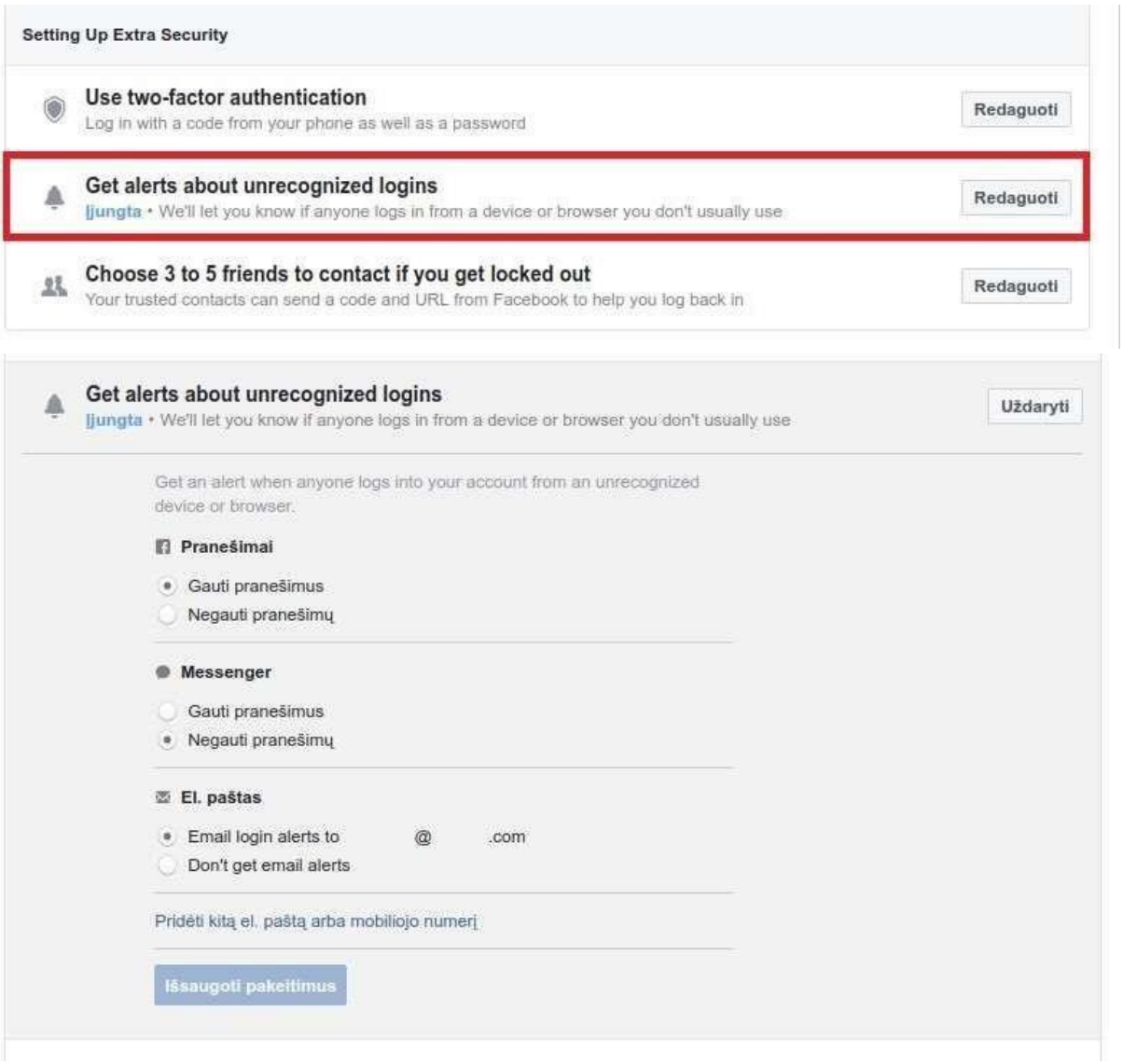
Anbefalinger om, hvordan man forhindrer indbrud

• Brug en sikker adgangskode (det anbefales, at adgangskoden består af mindst 9 tegn, inklusive store og små bogstaver, tal og tegnsætning);

- Giv ikke din adgangskode til nogen;
- Brug ikke den samme adgangskode, som du bruger til andre konti; Log ikke ind
- på din konto på offentlige enheder;
- Undgå at placere overdreven information på sociale netværk
- Brug tofaktorautentificering (Indstillinger ➔ Sikkerhed og logins)

Figur 2. Konfigurer tofaktorautentificering

• Indstil for at modtage e-mail. Underret dig om mislykkede login til din konto (Indstillinger ➔ Sikkerhed og logins).



Figur 3. Underretninger om mislykket login til din konto

Hvad skal jeg gøre, hvis jeg bemærker mistænkelig aktivitet eller mister min Facebook-konto? Hvis du har mistanke om, at tredjeparter har fået adgang til din konto:

• Skift dit kodeord så snart a *s* muligt;

• Kontroller for mistænkelige forbindelser (Indstillinger ➔ Security and Connections), frakobl følgende enheder, når du bemærkes:

Figur 4. De enheder, der er logget ind på din konto

• Hvis du ikke kan logge ind på din konto, skal du prøve at gendanne den ved hjælp af din e-mail.

• Du kan rapportere et mistet acco-uhntttps: //www.facebocookm . / hacket

• Hvis du ikke fejler din konto selv, kan du kontakte retshåndhævelse.

[Nøgleord: facebook, konto, private data, social sikring, anmeldelse].

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne offentliggørelse af [kommunikation] afspejler kun forfatterens synspunkter,

Denne paronjdedtbhaCsobmenisfsuionndecd anwniothbsuephpeoldrtrfersopntshieblEeufroorpaenaynuCsoemhisicshiom n.aTyhbisepmuabdliecaotfiotnhe [cionm formuantiicoantioconn] traeifnleecdtsththereevinie.ws kun af autoriteten eller, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.

GENERATION DATA

USING DATA FOR PROFIT

Casestudie med skadelige e-mails

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation [meddelelse] afspejler kun autoritetens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.

CYBERNET SIKKERHEDSCENTER UNDER FORSVARSMINISTERIET

SENDELSE TIL E-MAILEDE VIRKSOMHEDER I LITAUEN BREV MED SKADELIG SOFTWAREKODE

National Cyber Security Center under Ministeriet for National Defense (NKSC) oplyser, at i Litauen spreder e-mails med ondsindet kode. I de seneste dage registrerer NKSC tilfælde af forfalskning af e-mails fra kendte litauiske og udenlandske virksomheder, e-mail-adresser, deres logoer og kontaktoplysninger distribuerer ondsindet softwarekode.

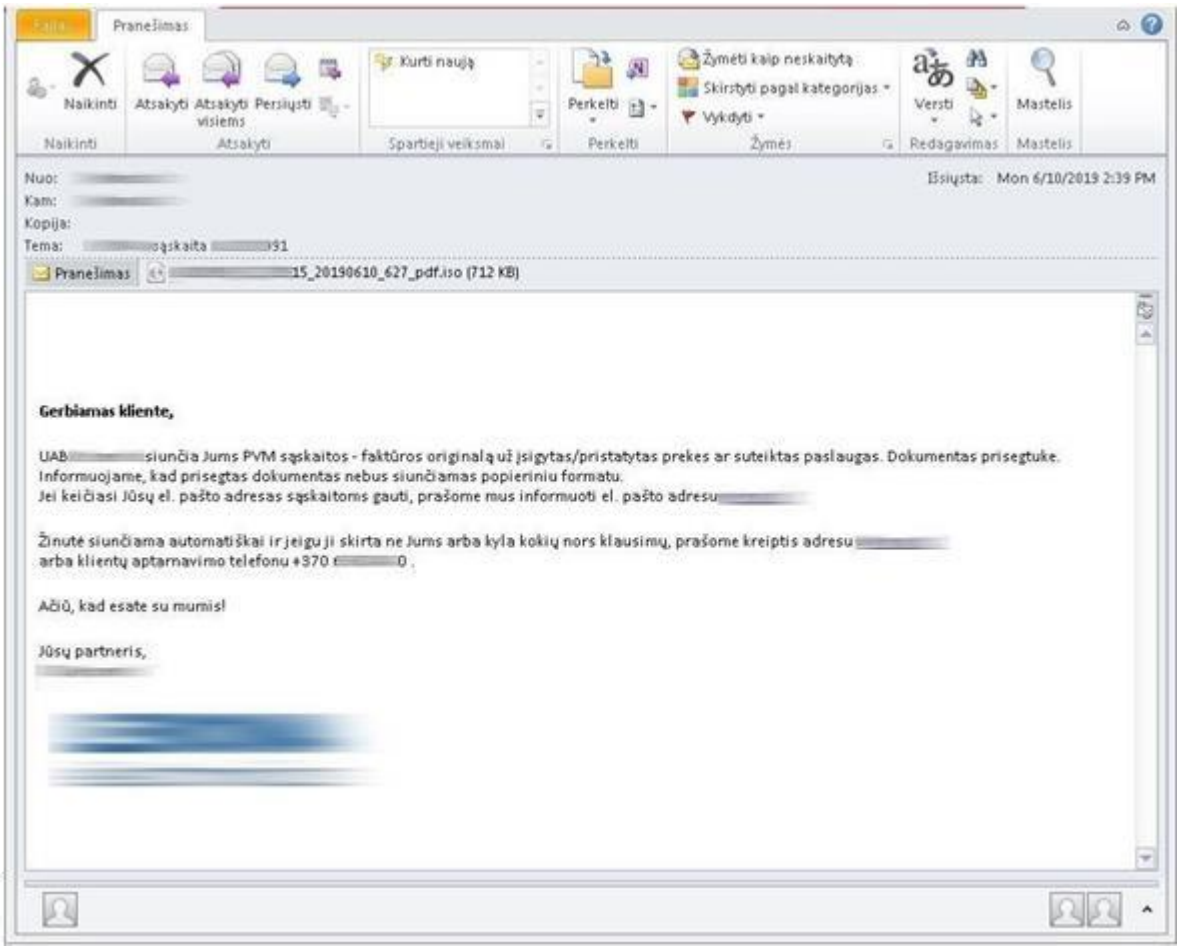


Fig. 1. Falsk e-mail et eksempel på et brev, der simulerer en leverandør

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation [meddelelse] afspejler kun autoritetens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.

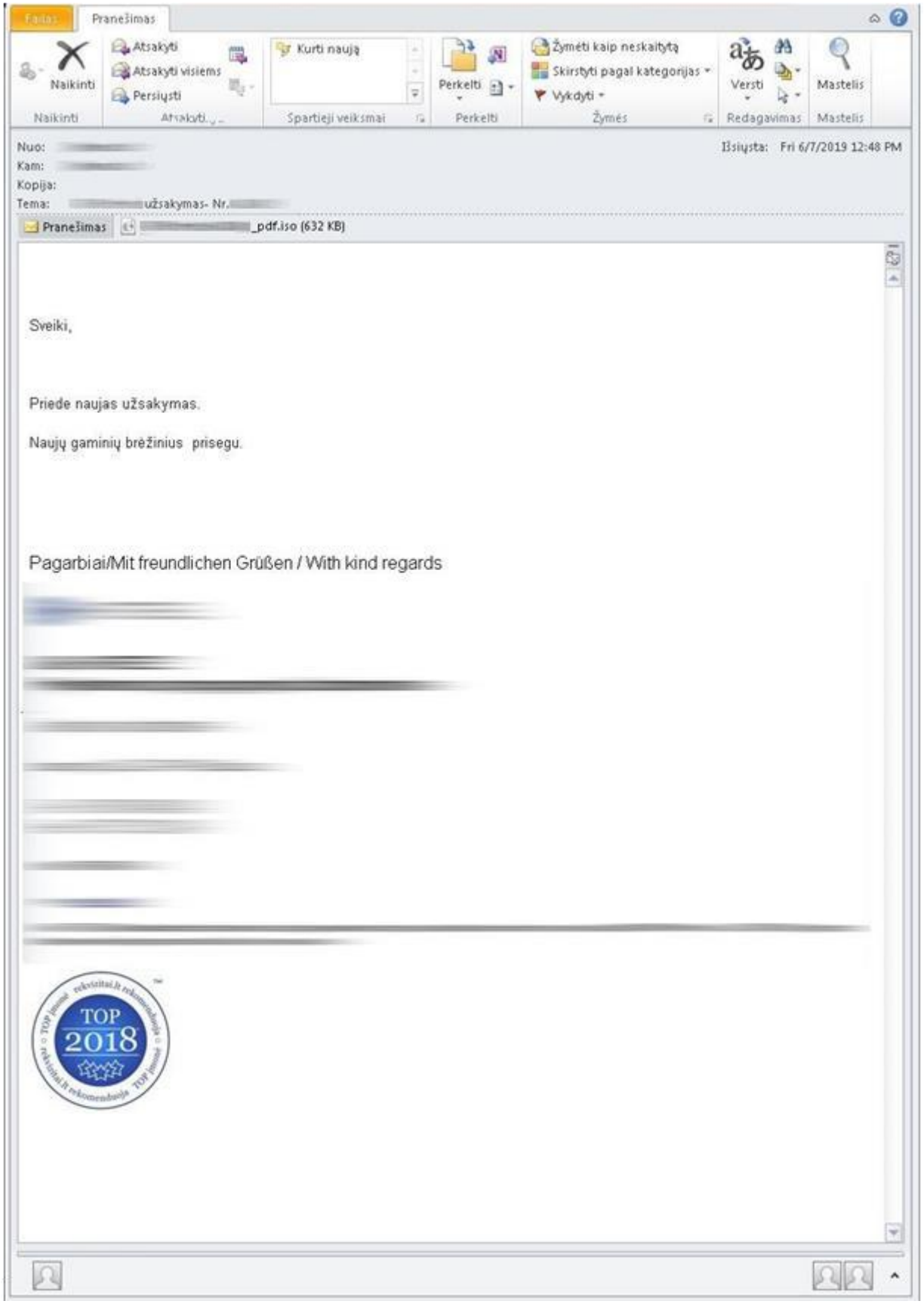


Fig. 2. Falsk e-mail et eksempel på et brev, der simulerer en leverandør

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation [meddelelse] afspejler kun autoritetens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.

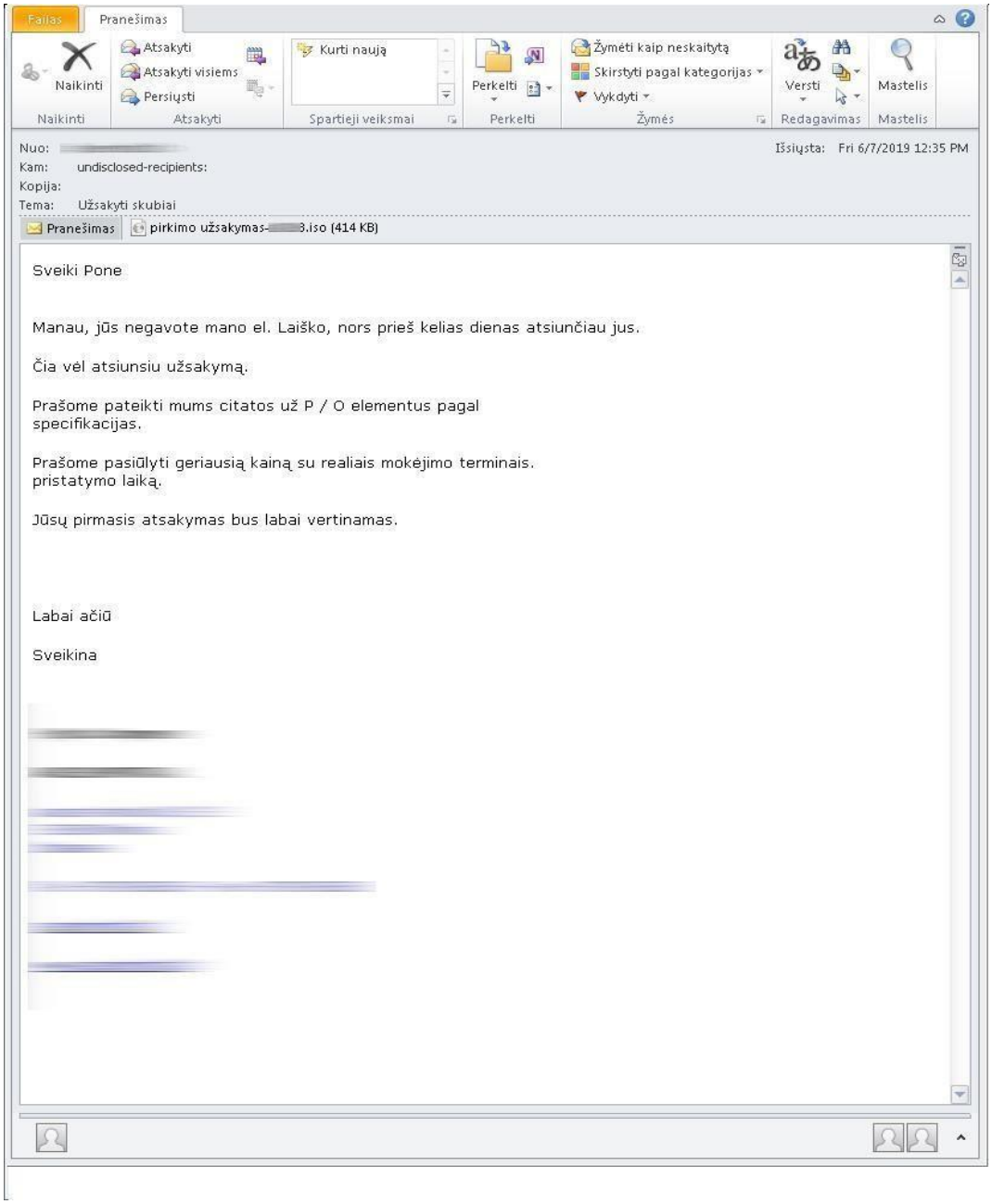


Fig. 3. Falsk e-mail et eksempel på et brev, der simulerer en leverandør

Den ondsindede kode hostes i * .iso-filer, der er knyttet til e-mail. Brev. Den vedhæftede fil indeholder den eksekverbare * .exe-fil. Når den vedhæftede fil åbnes, og * .exe-eksekverbarheden udføres, forsøger skadelig software at indsamle personlige brugeroplysninger fra computeren, henter computernavnet, forsøger at identificere, om computeren kan fås til fjernadgang (eller Remote Desktop-funktionalitet) og sender oplysninger til en ekstern server. station og andre efterretningsaktiviteter.

Teksten til brevet er normalt skrevet på litauisk. Meddelelsen virker realistisk for modtageren, da den sendes fra en kendt og betroet adressat, men faktisk er forfalsket.

Anbefalinger

Kontroller overskrifterne for meddelelsen for at se, hvem der er den virkelige afsender af meddelelsen (Fra feltet). Når man analyserer en header, skal man se på den første parameter modtaget fra bunden. Denne parameter fortæller dig fra hvilken server e-mailen blev sendt. brev. Hvis Fra-feltet er sender@imone.com , skal feltet Modtaget også vise adressedomænet (domæne) "imone.com". I tilfælde af denne fidus, feltet Modtaget

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation [meddelelse] afspejler kun autoritetens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.

viser en helt anden data end hvor meddelelsen blev sendt. Se også: Fig. 4.

Fig. 4. Falsk e-mail sand afsender af meddelelsen

Afhængigt af din e-mail-adresse til e-mail-klienter varierer muligheden for at se overskrifter. Bemærk, at cyberkriminelle regelmæssigt også distribuerer anden ondsindet kode, der udnytter sårbarheder i forskellige software, og vi anbefaler, at du regelmæssigt opdaterer dit antivirus, operativsystem og anden software, du bruger.

For at hjælpe med at forhindre spam anbefaler vi, at du aktiverer og korrekt konfigurerer SPF (Sender Policy Framework) -funktionalitet for at spam e-mail-kontakter. Denne funktion skal bruges med ekstra forsigtighed, da forkerte indstillinger kan få nogle meddelelser til deres modtagere.

Som en påmindelse er nøglen at være konstant opmærksom og kritisk over for indgående mail.

[Nøgleord: falsk e-mail, ondsindet softwarekode, spam].

Dette projekt er blevet finansieret med støtte fra Europa-Kommissionen. Denne publikation [meddelelse] afspejler kun autoritetens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der kan gøres af oplysningerne deri.