Cybersave Yourself

René Ritzen
Corporate Information Security Officer

Utrecht University

CYBERSECURITY AWARENESS

Informtiebeveiliging belangrijk?

- Informatiebeveiliging en Privacy is duur
- Terugverdientijd is laag
- Risico’s lijken acceptabel
- Liever investeren in primaire proces

Datalekken


Hogeschool versp
9 maart 2016
Hogeschool Van Hall Lare
doorgestuurd naar alle stud
BSN-nummer van studenten
Dit meldt Omroep Gelderland.
Publeaks, waar mensen anonie
Studenten van de Radboud
interne netwerk kampte met een beve
salarissen van medewerkers op straa
van personeel en studenten.
Gegevens bijna 800 kankerpatiënten gestolen
3 maart 2016 om 16:42 door Astrid Ottens
2
0
0
NKI-AVL
Het Nederlands Kanker Instituut
Antoni van Leeuwenhoek Ziekenhuis
Het Antoni van Leeuwenhoek. Foto: ANP
Dieven hebben een onbeveiligde harde schijf gestolen met de gegevens van 781 kankerpatiënten van het Antoni van Leeuwenhoek Ziekenhuis. De schijf is in december uit de kofferbak van de auto van een onderzoeker gestolen. Dat maakte het Amsterdamse ziekenhuis donderdag bekend.
tudenten
SERVICE
n per ongeluk
s, -mailadressen en het

Identiteitsfraude

CSY

Datamanipulatie

Tentamenfraude HHS

07-02-2014 | 16:27

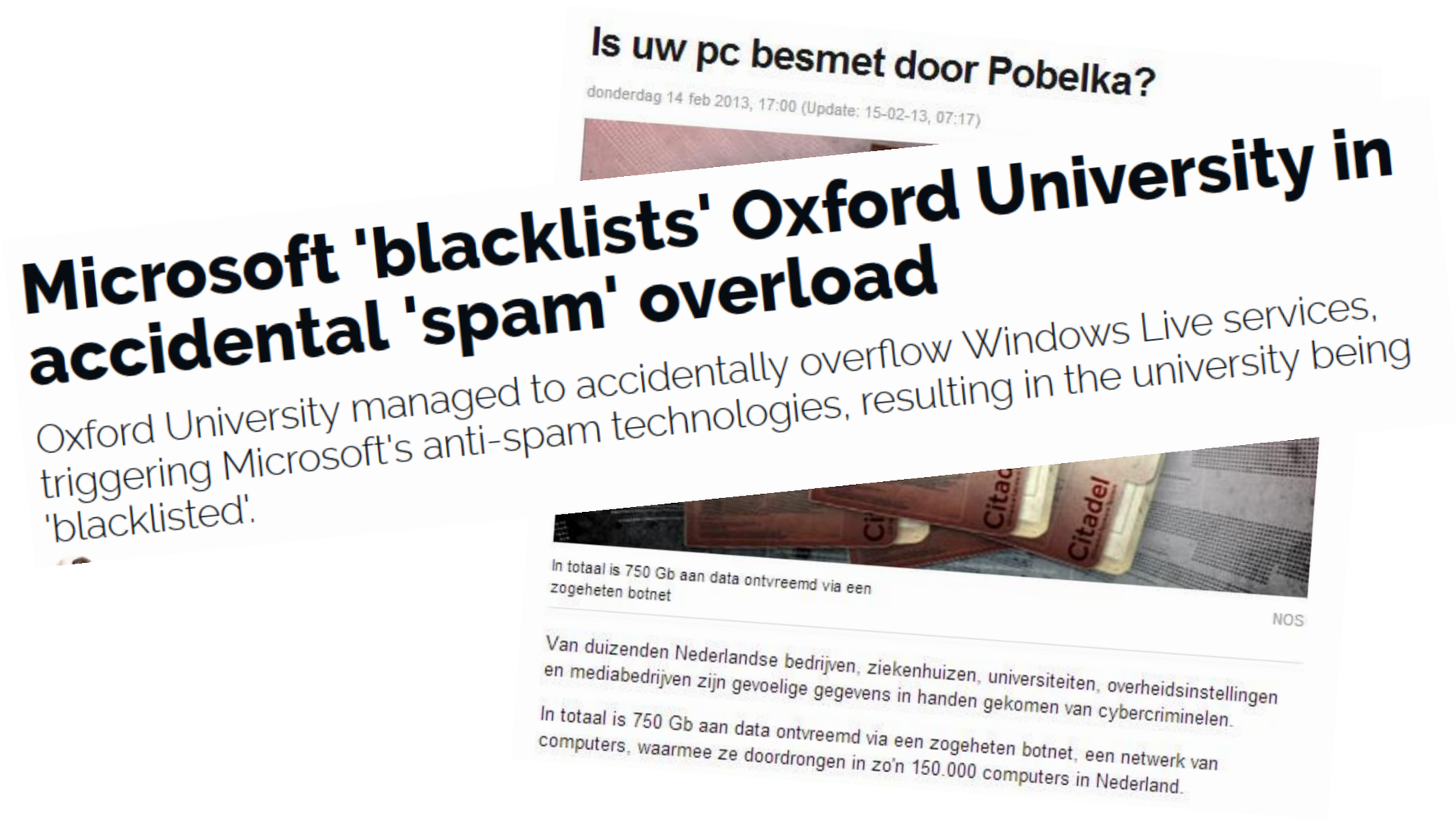
2

Op de Haagse Hogeschool wordt waarschijnlijk flink gesjoemeld met tentamens. Studenten weten van tevoren de hand te leggen op tentamenvragen en hoeven alleen nog maar de antwoorden uit hun hoofd te leren, zo blijkt uit informatie van Omroep West. De directie van de Haagse Hogeschool laat nu onafhankelijk onderzoek doen naar mogelijke tentamenfraude.

Spionage


© REUTERS
Nederlands-Duits defensiebedrijf gehackt door Chinezen
Het Nederlands-Duitse bedrijf Rheinmetall Defence is vanaf 2012 aangevallen door een groep Chinese hackers. Die hebben daarbij 'zeker' toegang gekregen tot technologische informatie van het bedrijf en hadden waarschijnlijk tot voor kort controle over het bedrijfsnetwerk. De hackers kwamen binnen door een aanval op het Duitse bedrijf, waardoor ook Nederlandse informatie binnen handbereik kwam. Dat bevestigen bronnen in de inlichtingenwereld aan de Volkskrant.
Door: Huib Modderkolk 15 juni 2016, 02:00
NEWS
iversity of Virginia will spend millions on new
ity after Chinese hack
present in University server since Spring 2014
h Hall | Sep 16 2015 | 09/16/15 10:23pm
Pin it
r its information
lune data
more

Misbruik van ICT-voorzieningen



Is uw pc besmet door Pobelka?

donderdag 14 feb 2013, 17:00 (Update: 15-02-13, 07:17)

Microsoft 'blacklists' Oxford University in accidental 'spam' overload

Oxford University managed to accidentally overflow Windows Live services, triggering Microsoft's anti-spam technologies, resulting in the university being 'blacklisted'.

In totaal is 750 Gb aan data ontvreemd via een zogeheten botnet

NOS

Van duizenden Nederlandse bedrijven, ziekenhuizen, universiteiten, overheidsinstellingen en mediabedrijven zijn gevoelige gegevens in handen gekomen van cybercriminelen.

In totaal is 750 Gb aan data ontvreemd via een zogeheten botnet, een netwerk van computers, waarmee ze doordrongen in zo'n 150.000 computers in Nederland.

Verstoring Infrastructuur

Websites Universiteit Leid door ddos-aanval

Gepubliceerd: 06 oktober 2015 14:17
Laatste update: 06 oktober 2015 21:33

De websites van Universiteit Leiden was o ddos-aanval.

Dat meldde de universiteit dinsdag.

De ddos-aanval werd dinsdagmiddag geconstatee avond waren opgelost. Er wordt nog onderzocht of met de dreiging van dinsdag.

Vrije Universiteit Amsterdam getroffen door cryptolocker-virus

Door Joost Schellevis, maandag 9 maart 2015 14:32, 101 reacties, 13.069 views • Feedback

In de afgelopen week zijn circa 200 computers van de Vrije Universiteit Amsterdam getroffen door Cryptolocker, malware die bestanden versleutelt en tegen betaling weer ontsleutelt. Volgens de VU zijn nog geen bestanden verloren gegaan als gevolg van de infectie.

Woordvoerster Aukje Schep bevestigde de infectie, nadat beveiligingsonderzoeker Rickey Gevers een screenshot van een mededeling van de VU postte op Twitter. De waarschuwing roept studenten en medewerkers op om niet zomaar bijlagen in e-mails te openen. Ook op linkjes mag niet zomaar worden geklikt, waarschuwt de Vrije Universiteit.

Volgens woordvoerster Schep begon de relatief grootschalige infectie een week geleden en zijn er in die periode 'om en nabij' tweehonderd computers geïnfecteerd. "De malware waart al wel een tijdje rond, de afgelopen maanden werden af en toe al pc's geïnfecteerd", zegt Schep. Waardoor het aantal aanvallen zo is toegenomen, weet Schep niet. "We hebben nog geen idee in welke hoek we dit moeten zoeken."

De zogeheten ransomware versleutelt bestanden en eist dat gebruikers betalen voordat ze weer worden ontsleuteld. "Maar wij betalen natuurlijk niet", aldus Schep. De universiteit stelt dat er voor zover bekend bovendien nog geen bestanden verloren zijn gegaan door de malware-infectie.

CSY

Grootste bedreigingen voor Onderwijs en Onderzoek

- Datalekken
- Identiteitsfraude
- Datamanipulatie
- Spionage
- Verstoring van ICT-infrastructuur
- Misbruik van ICT-voorzieningen
- Bewust imagoschade

Risico’s

- Imagoschade
- Verlies van intellectueel eigendom
- Verstoring primaire processen
- Hoge kosten schadeherstel
- Non-compliance
- Persoonlijke schade

En het risico wordt groter...


'Cybercrime kost Nederland jaarlijks 10 miljard'

MA 4 APRIL, 00:13 BINNENLAND, ECONOMIE, TECH


nieuwsuur

'Over vijf jaar helft misdaad door cybercriminelen'

WOENSDAG, 16:46 BINNENLAND


NOS Nieuws Sport Uitzendingen

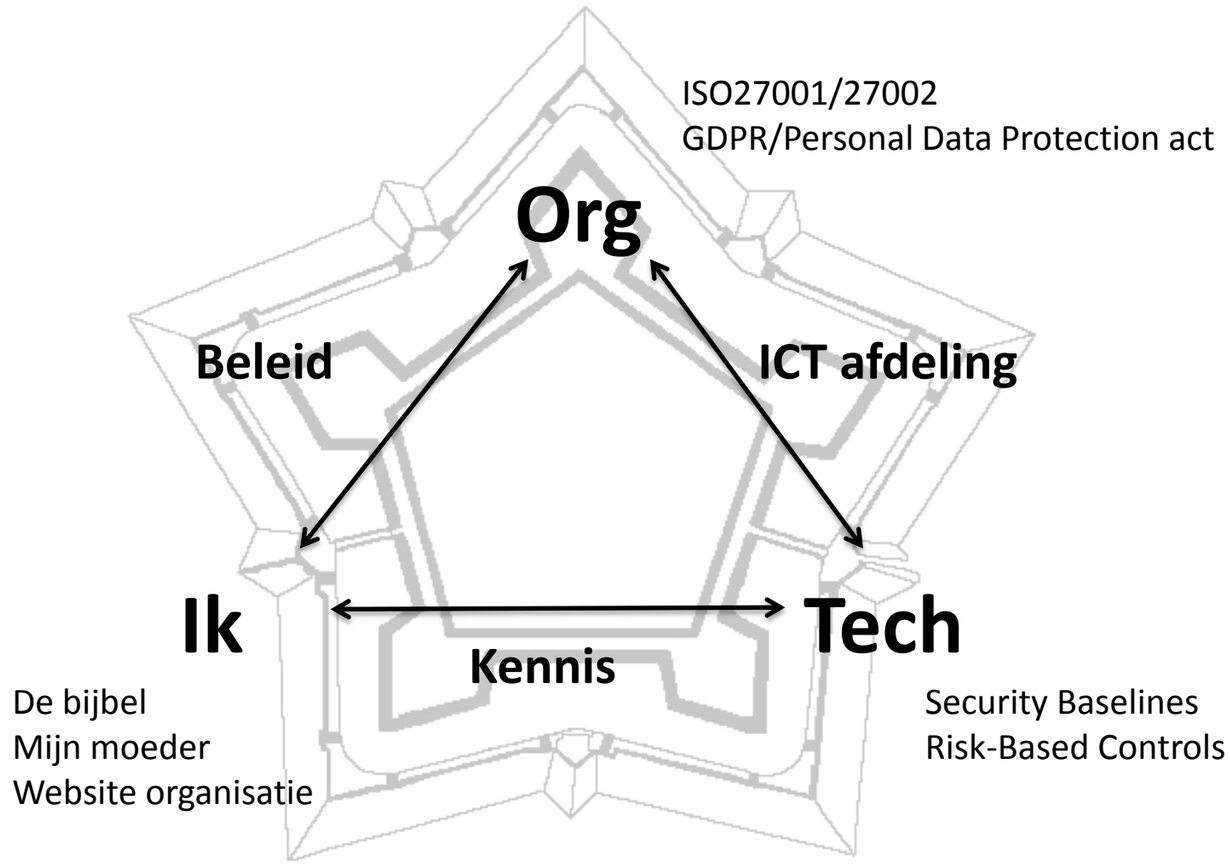
2 GERELATEERDE ARTIKELEN

Dijkhoff: cybercrime begint economie te raken

11-04-2015, 11:04 POLITIEK

CSY

Wat kun je doen?



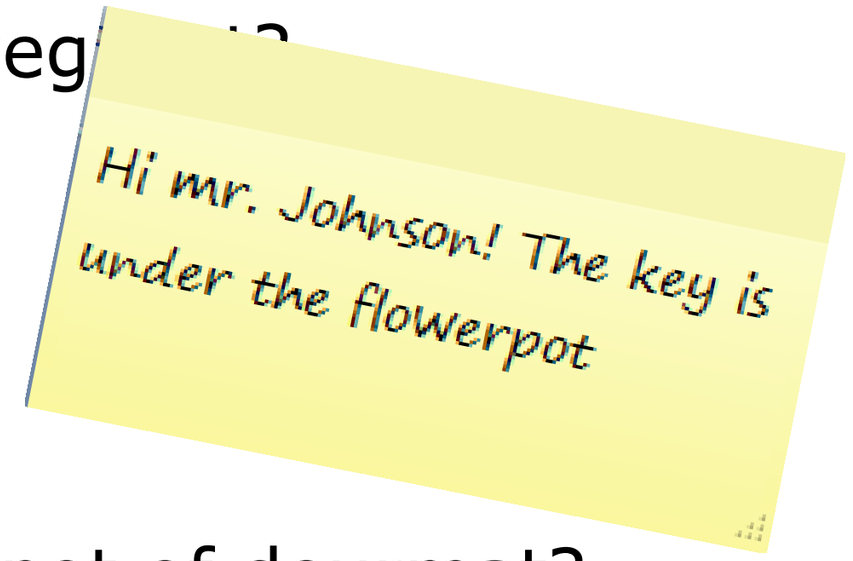
https://www.youtube.com/watch?v=opRMrEfAIiI

De zwakste schakel

- Gebrek aan risicobewustzijn
- Gebrek aan bewustzijn van verantwoordelijkheden
- Gebrek aan empowerment
- Eigen beoordeling faalt
- Mensen maken nu eenmaal fouten…

Ik? Hoezo?

- Wie doet de deur op slot wanneer je weg
- De achterdeur ook?
- Wie laat waardevolle spullen in zicht?
- Wie heeft een sleutel onder een bloempot of deurmat?
- Wie hangt een briefje naast de deurbel?



Inbraken

2012	Huishoudens	
# in NL	8.000.000	
# inbraken	92.000	
Kans op inbraak	1,2%	
Gemiddelde schade	€ 1.800	
Totale schade NL	€ 165.600.000	
Gemiddelde tijd detectie	10 minuten	
Kans dat nu iemand inbreekt	0,00001%	

Inbraken

2012	Huishoudens	Computers
# in NL	8.000.000	10.000.000
# inbraken	92.000	1.000.000
Kans op inbraak	1,2%	10%
Gemiddelde schade	€ 1.800	€ 300
Totale schade NL	€ 165.600.000	€ 300.000.000
Gemiddelde tijd detectie	10 minuten	36 days
Kans dat nu iemand inbreekt	0,00001%	1%

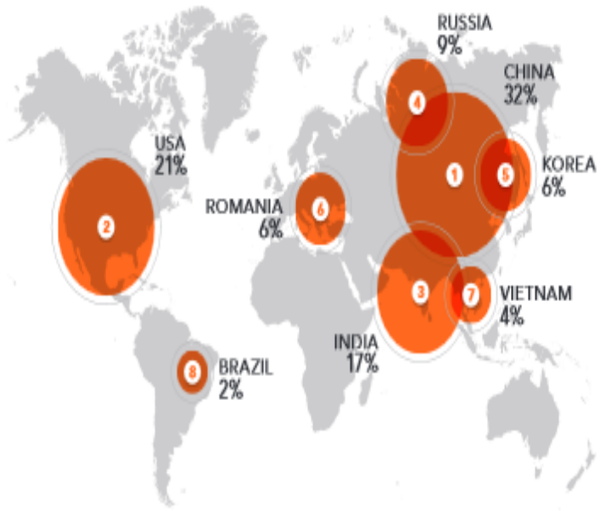
Bron: Prof. Eric Verheul, Inaugural address, Januari 2014

Herken de boef

» USA

Origin of Attack

Attacks on US targets most frequently come from China, the US, India and Russia.



Type of Malware

94% of malware observed was credential-stealing malware.

 # accounts compromised

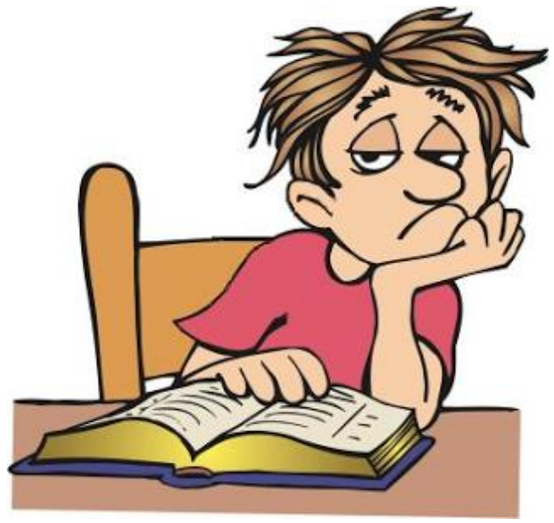
MySpace:	360 miljoen
VK.com:	171 miljoen
LinkedIn:	117 miljoen
Tumblr:	65 miljoen
Mail.ru:	57 miljoen
iMesh:	51 miljoen
Yahoo Mail:	40 miljoen
Hotmail:	33 miljoen
Twitter:	32 miljoen
Mate1:	27 miljoen

Source: Volkskrant June 14 2016

CSY

Zo lossen we het op, toch?

- Regels en beleid aankondigen
- Een website! Daar leren ze van!
- Nieuwbrieven en nog eens nieuwsbrieven
- Campagnes met leuke gadgets
- Posters!



Wie heeft:

- Regels en beleid
- Een website
- Nieuwbrieven
- Campagnes
- Posters

Effectiviteit

Wie herinnert zich nog de laatste security awareness campagne bij je eigen organisatie?

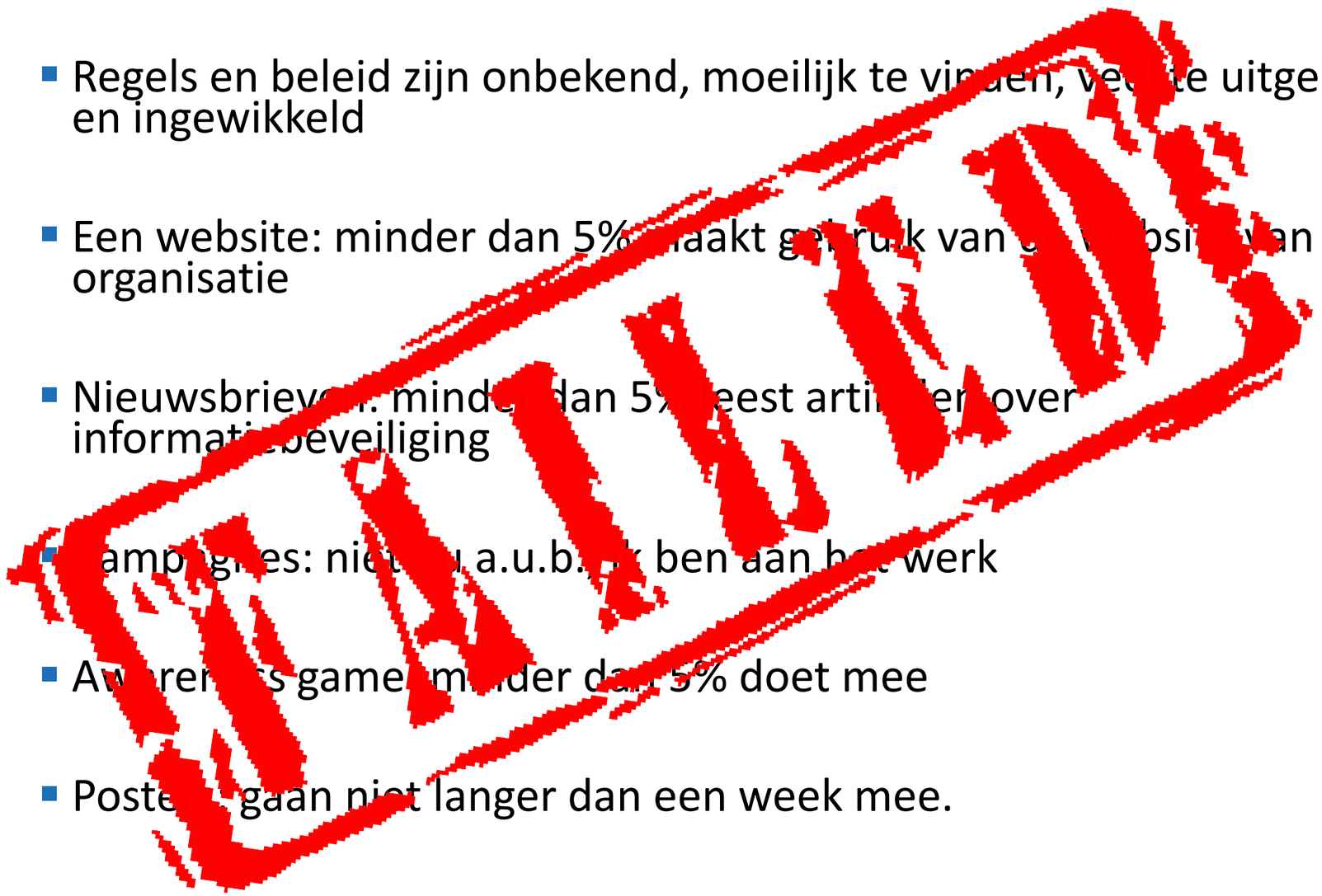
Waar ging het over?

Wat was het resultaat?

- Was heel effectief!
- Nou…
- Had niet het gewenste effect

Wat vaak gebeurt…

- Regels en beleid zijn onbekend, moeilijk te vinden, veel te uitgebreid en ingewikkeld
- Een website: minder dan 5% maakt gebruik van de website van hun organisatie
- Nieuwsbrieven: minder dan 5% leest artikelen over informatiebeveiliging
- Campagnes: niet nu a.u.b. ik ben aan het werk
- Awareness games: minder dan 5% doet mee
- Posters gaan niet langer dan een week mee.



De profeet en de berg

"If the mountain will not come to the prophet, the prophet must go to the mountain"

- Communicatiemiddelen zijn belangrijk, maar op zichzelf ineffectief

- We kunnen er niet op vertrouwen dat gebruikers het uit zichzelf goed doen.

- Als breed uittoeteren (broadcasting) niet werkt, moeten we naar gericht communiceren schakelen (narrowcasting)

Er is niet zo iets als DE gebruiker

- Herken verschillen en benader ze in hun eigen context: management, docenten, onderzoekers, staf, studenten, etc.

- Leer van hun problemen en dagelijkse gewoonten

- Heb het over risico’s die relevant zijn en gebaseerd op de werkelijkheid; hoe ze te herkennen en de impact te vermijden

- Maak bondgenoten, niet tegenstanders

Do’s and Dont’s

DO	DON’T
Werk in de juiste context	*One size fits all* advies
Richt je op het gebruikersperspectief	Organisatiebrede campagnes
Promoot best practices en beschrijf ze indien nodig	’Mag niet’ benadrukken
Beloon goed gedrag	Alleen maar benoemen wat fout gaat
Suboptimaal gedrag is beter dan ontwijkgedrag	Regel zijn regels
Stimuleer zelfregulering en lokale protocollen die verbonden zijn met de dagelijkse praktijk	
Leer van fouten en incidenten en wees transparant	
Maak gebruik van de actualiteit als kapstok	
Vorm bondgenootschappen met stakeholders	

THINK BIG

ACT SMALL

EN BEGIN VANDAAG!

COMMUNITY AS A SERVICE

IB&P Community voor Onderwijs en Onderzoek

- Intensieve samenwerking in community gebaseerd op vertrouwen

- Samen ontwikkelen van nieuwe materialen en aanpak (games, e-learning modules)

- Delen van ervaringen: successen en mislukkingen

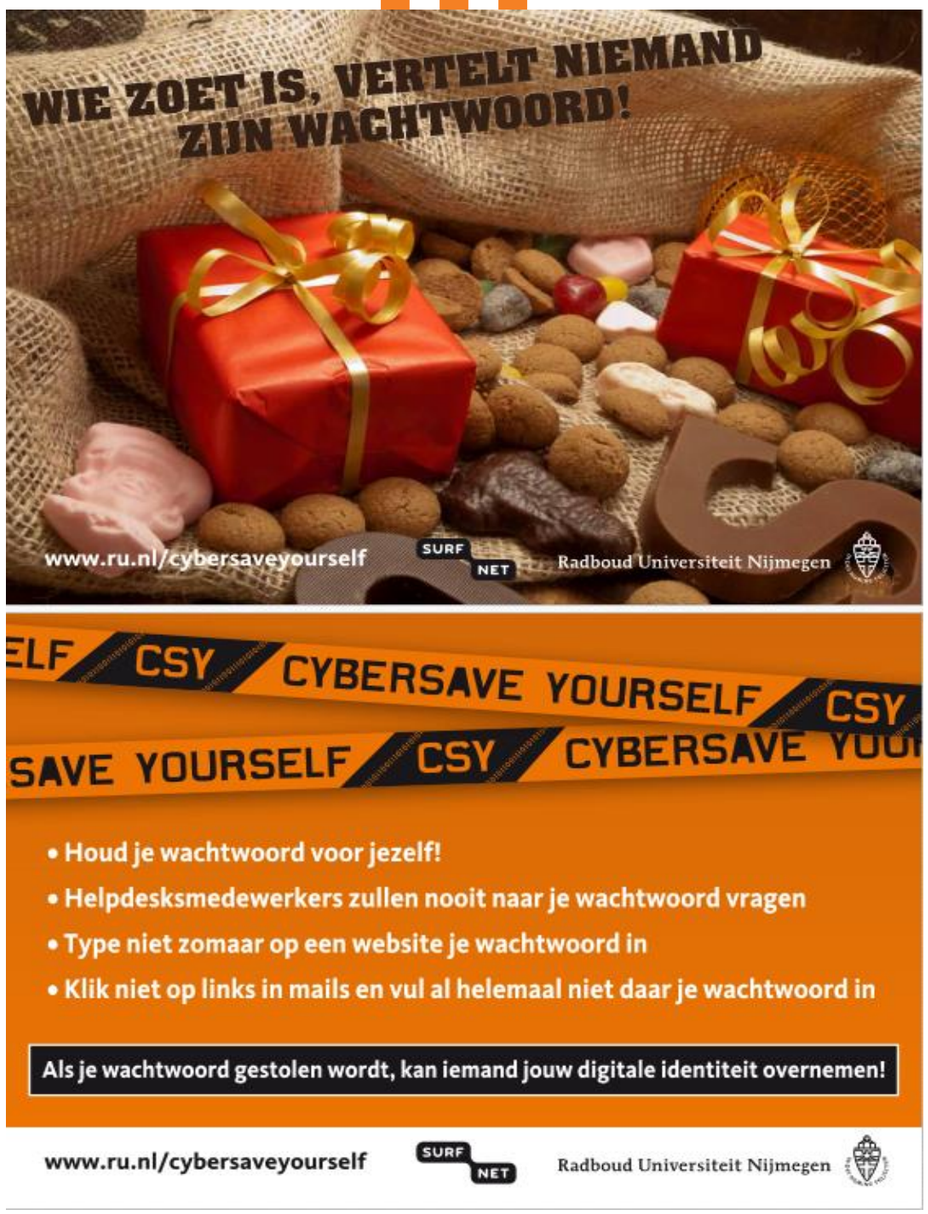
- Cybersave Yourself
  - Als een bron van middelen: de toolkit
  - Als een bron van informatie: de knowledge base

Voorbeeld:
Smart Secure Yourself

Voorbeeld: Your babies

Voorbeeld: encryption week

Voorbeeld: Wie zoet is …



Een nieuwe strategie voor Awareness

- In een open en pluriforme omgeving zoals in O&O kunnen we niet vertrouwen op beleidstukken en technische oplossingen alleen.

- Gebruikers moeten zelf risicoafwegingen kunnen maken en op deze verantwoordelijkheid gewezen worden.

- Wanneer een strikte regel of beleid van toepassing is: leg uit waarom! Acceptatie begint met begrip.

- Management op alle lagen moet aandacht hebben voor privacy en security:
  - Geef het goede voorbeeld en implementeer best practices
  - Toon leiderschap in het voltooien van culturele en gedragsverandering.
  - Laat zien dat security en privacy belangrijke onderwerpen zijn in de bestuurskamer.

CYBERSAVE YOURSELF

Wat is Cybersave Yourself?

- Cybersave Yourself is een SURFnet-dienst voor onderwijs- en onderzoeksinstellingen die een bewustzijnscampagne willen opzetten op het gebied van informatiebeveiliging en privacy

- De dienst is gericht op security officers en communicatie-medewerkers en biedt hen allerlei middelen en handleidingen om het bewustzijn binnen de eigen organisatie te vergroten

- De dienst bestaat uit een toolkit waar alle middelen beschikbaar zijn en een website (nog in ontwikkeling) waar content beschikbaar is

Insteek / concept

Insteek
- Centrale inzicht: digitale onveiligheid ‘dichterbij is dan je denkt’
- Doel is om mensen op verschillende manieren bewust maken van (cyber)risico's zodat ze zelf hierin keuzes kunnen maken

Concept
- Het concept bestaat uit het introduceren van nieuwe (niet bestaande) woorden
- Elk woord is combinatie van een bedreiging/risico met een persoon/situatie uit de directe omgeving
- Woord werkt vervreemdend waardoor lezer openstaat voor adviezen

Bewust maken van risico is:
- Mensen of situatie in de buurt (e.g. kantine, studieruimte)
- Technische kennis is niet nodig voor cybercriminaliteit (het is makkelijk)
- Motieven zijn divers, van financieel gewin tot pesterijen
- Kortom: het kan iedereen overkomen

Voorbeeld: meekijkwifi

Onderwerp
Openbare wifi-netwerken

Begeleidende tekst
Je account overgenomen! Zonder dat je het doorhebt. Want je maakt maar wat graag gebruik van een gratis en openbaar netwerk. Wist jij veel dat het een meekijkwifi was. En dat andere wifi-gebruikers dan heel makkelijk kunnen zien wat je doet, waar je inlogt en welke toetsen je dan aanslaat.

Wees je bewust van meekijkwifi’s. Ga voor tips naar cybersaveyourself.nl

Start: 4 onderwerpen

CSY

Middelen / flexibiliteit

De toolkit is zeer flexibel opgezet, de meeste middelen zijn volledig bewerkbaar.

U kunt bijvoorbeeld:
- Gebruik maken van kant en klaar materiaal
- Uw logo op de middelen plaatsen
- Materialen aanpassen aan eigen huis- of campagnestijl

Beschikbare middelen

- *Templates voor*
  - *Advertenties*
  - *Flyers*
  - *Koffiebekers*
  - *Krantenpagina*
  - *Placemats*
  - *Posters*
  - *Schermafbeeldingen*
  - *Spiegelstickers*

- *Game: Smart Secure Yourself*

- *Cyberstellingen over Privacy (+ template)*
- *Overkoepelende materialen waaronder draaiboek voor opzetten campagne*

Uitwerking van poster

Je account overgenomen! Zonder dat je het doorhebt. Want je logt maar wat graag in op een gratis en openbaar netwerk. Wist jij veel dat het een meekijkwifi was. En dat andere wifi-gebruikers dan heel makkelijk kunnen zien wat je doet, waar je inlogt en welke toetsen je dan aanslaat.

WEES JE BEWUST VAN MEEKIJKWIFI'S. GA VOOR TIPS NAAR
CYBERSAVE YOURSELF.NL

CSY

Utrecht University

CSY

Blik op toekomst

- Nieuwe website
- Onderwerpen voor specifieke doelgroepen toevoegen
- Meer actieve middelen (e.g. games, tests, workshopmateriaal, etc.)
- Samen met instellingen nieuw campagnemateriaal ontwikkelen, bijv:
    - Nieuwe onderwerpen
    - Studentenprojecten
    - Nieuwsredactie

Aan de slag en doe mee!

Toolkit met materiaal: https://wiki.surfnet.nl/display/CSY/

Website met tips: https://cybersaveyourself.nl
(nieuwe website volgt eind 2016 / begin 2017)

Vragen, suggesties, feedback: info@cybersaveyourself.nl

Doe mee!

- Maak zelf nieuwe materialen en deel het met ons
- Verzin nieuwe woorden en stuur ze in
- Deel campagne-ervaringen met ons

CSY