PROVINCIE :: UTRECHT

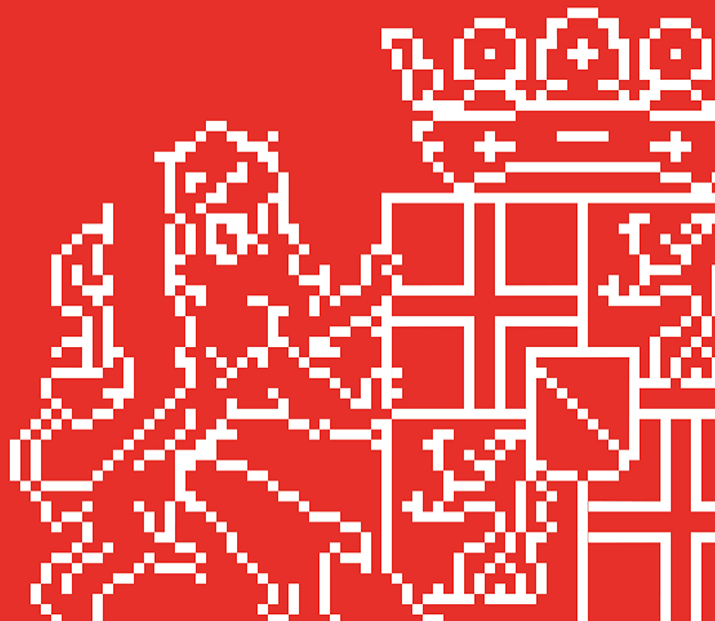
PRIVACY EN INFORMATIEBEVEILIGING IN DE PRAKTIJK

PROVINCIE UTRECHT

WIE ZIJN WIJ?

ELLEN KREMERS – PRIVACY OFFICER

JOHAN VAN MIDDELKOOP – CISO



De praktijk van de AVG en Informatiebeveiliging

Wat houden deze onderwerpen in?

Waar raken deze onderwerpen jouw werk als statenlid?

Informatiebeveiliging versus de AVG

Ziet op alle gegevens binnen een organisatie.	Ziet alleen op de gegevens die (in)direct herleidbaar zijn tot personen.
Gericht op de specifieke risico's voor een organisatie	Gericht op het beperken van de risico's voor personen.
Geen concrete wetgeving *	Europese verordening
Geen meldplicht bij datalekken *	Wettelijke meldplicht bij datalekken
Geen toezichthouder *	Toezicht door Autoriteit Persoonsgegevens

* Behoudens organisaties die zijn aangemerkt als "vitale aanbieder".

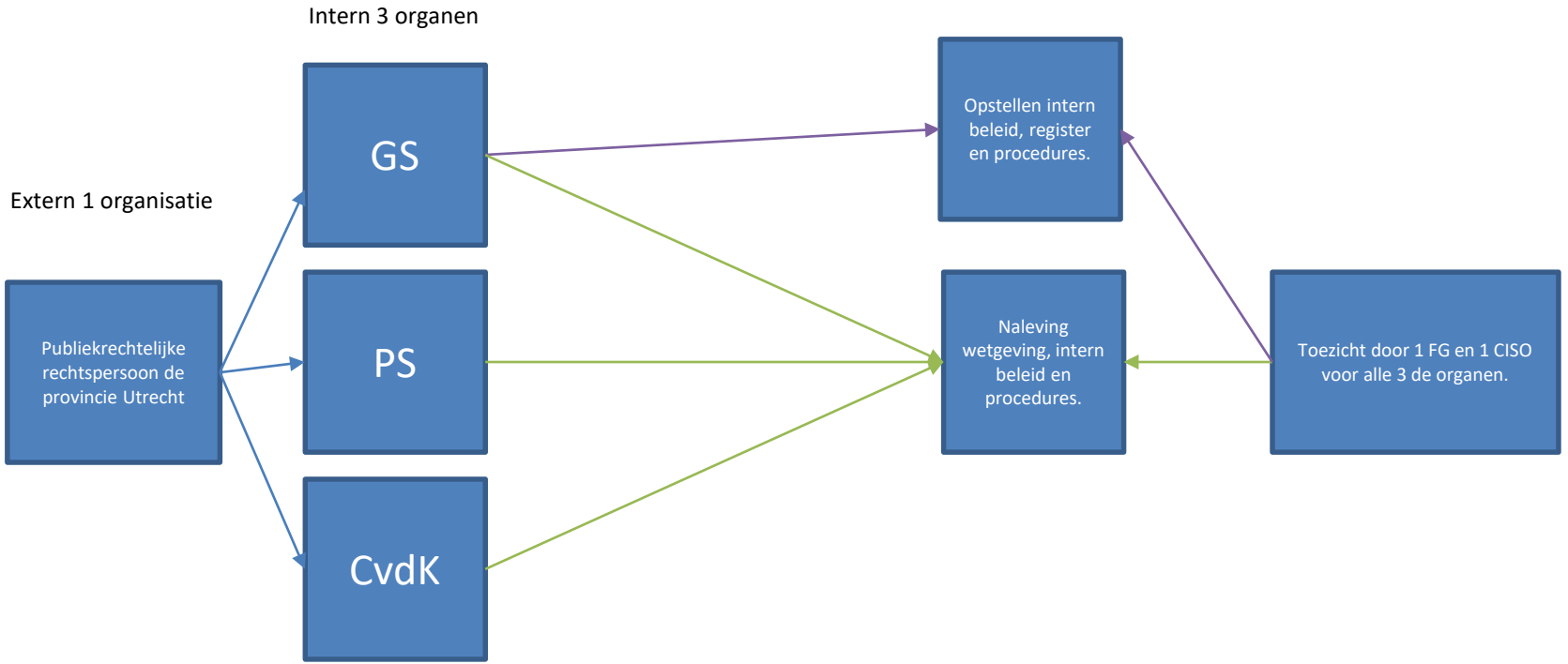
Grootste misverstanden omtrent de AVG

- Het mag niet (meer) vanwege de AVG.
- Je moet altijd toestemming vragen.
- Je mag persoonsgegevens niet delen met derden.

AVG is een “compliance” wet

- Verantwoording kunnen afleggen (d.m.v. register, beleid en procedures);
- Dataminimalisatie
- Verwijderplicht i.p.v. bewaarplicht.
- Zorgvuldig, actueel en goed beveiligen.
- Rechten betrokken kunnen nakomen.
- Informatieplicht
- Data Protection Impact Assessments
- Contracten

Informatiebeveiliging en AVG binnen de provincie Utrecht



Een datalek!

Wanneer is er sprake van een interne meldplicht bij een datalek?

Is er sprake van de volgende situatie?	En zijn de volgende soort gegevens daarbij betrokken?
Verkeerd verzonden, verlies, diefstal, toegang door onbevoegden en beveiligingsinbreuken zoals virussen, malware, hackers enz.	1. persoonsgegevens, en/of 2. vertrouwelijke informatie (bv gevoelige dossiers, bedrijfs- of concurrentie gevoelige informatie)

Wat te doen bij een vermoeden van een datalek? Stuur een bericht naar datalek@provincie-utrecht.nl

Waarom? Wij coördineren het volgen van de juiste procedures, wettelijke meldplicht, het beperken van eventuele schade en de communicatie.

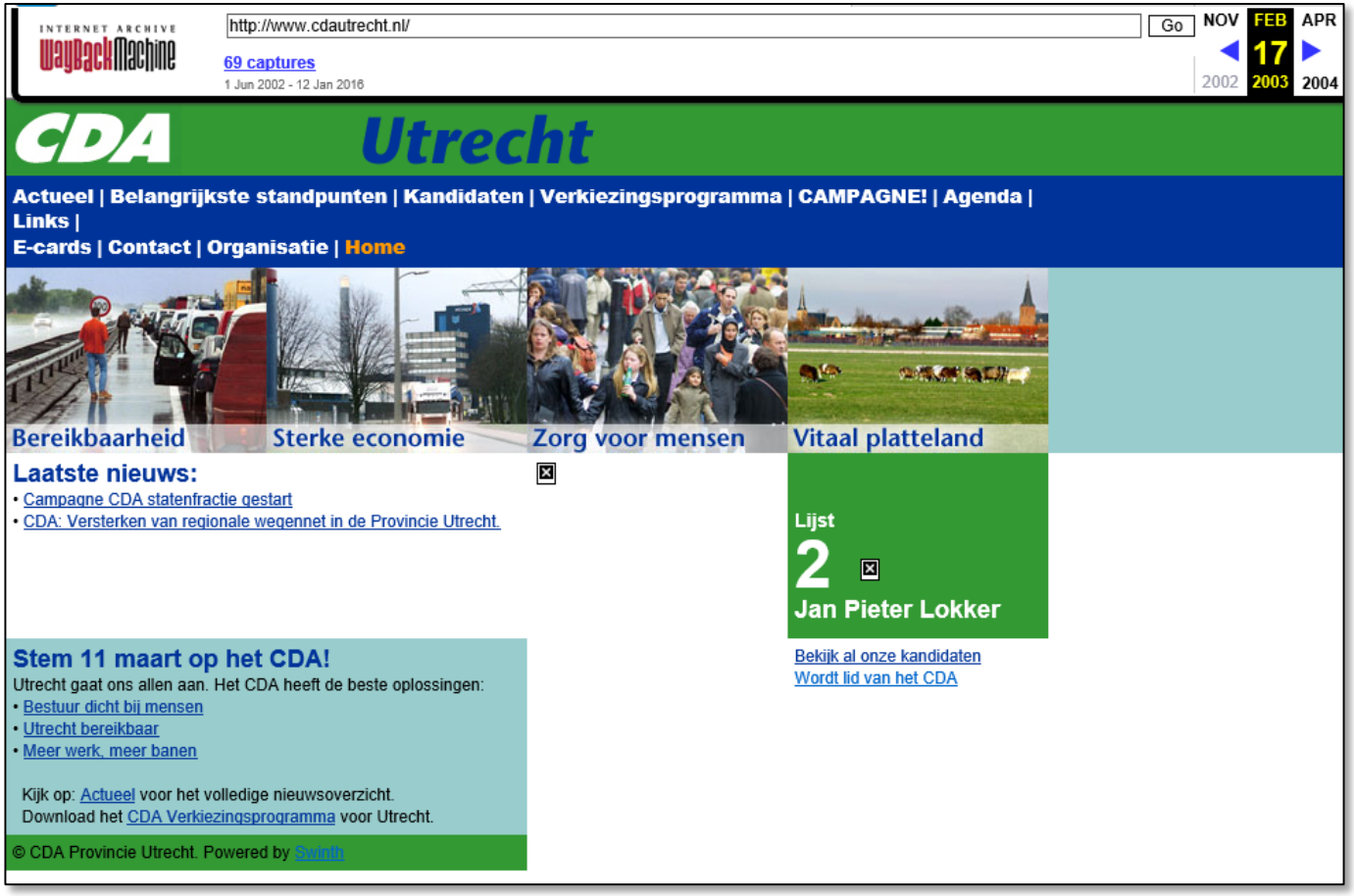
Waar kan ik als statenlid verder op letten?

van de Corporate Information Security Officer

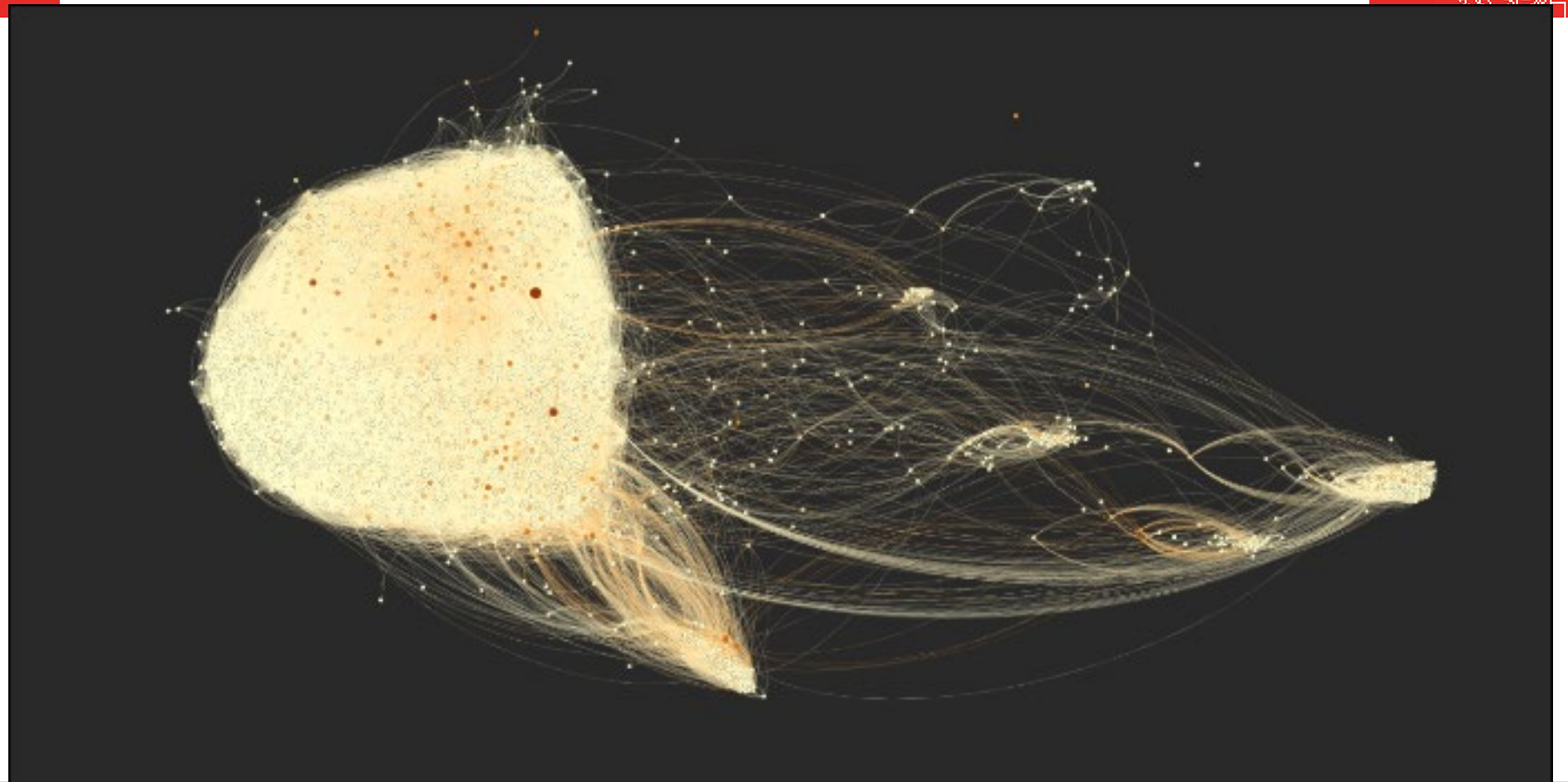
Waarom ben je interessant?

- ✓ Toegang tot geheime informatie
  - ✓ Gevoelige onderzoeken (Uithoflijn en Dolderseweg)
  - ✓ Bestemmingsplannen etc.
- ✓ Beïnvloeding van (politieke) besluitvorming
- ✓ Mensen in diskrediet brengen

Terug in de tijd…



Waar kan ik je vinden?



Waar kan ik je vinden?

Feiten:

- ✓ Social media = LinkedIn, Facebook, Pinterest, Instagram
- ✓ Hackers en kwaadwillenden zoeken graag in sociale media op zoek naar informatie
- ✓ Berichten blijven voor altijd bewaard

(WhatsApp, SMS etc zijn WOBbaar)

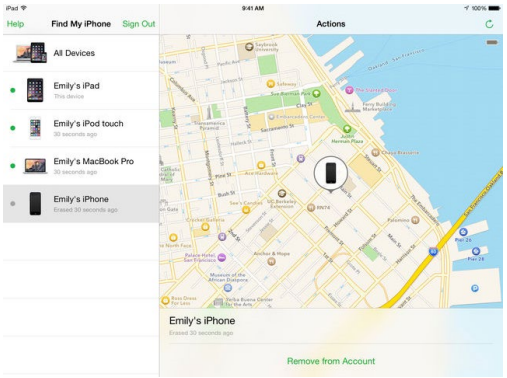
Tips:

- ✓ Zet je Facebook, LinkedIn of Instagram account op Privé waar mogelijk
- ✓ Verwijder regelmatig “oude” foto’s of berichten
- ✓ Deel geen foto’s met gevoelige informatie zoals brieven met namen, rijbewijs, pasjes, sleutels
- ✓ Hou privé gegevens privé

Mooi die iPad van de provincie

- ✓ Office 365
- ✓ Mail account
- ✓ Agenda
- ✓ Contacten
- ✓ OneDrive (bestanden delen *binnen* provincie)
- ✓ Staten informatie systeem (2 factor authenticatie)

Mooi die iPad van de provincie



- ✓ iPad is versleuteld
- ✓ Inloggen met code
  - ✓ 5 inlogpogingen
- ✓ Let op onvertrouwde apps
- ✓ Bij verlies of diefstal melden
  - ✓ doe aangifte in geval van diefstal
- ✓ Via iCloud zoeken naar iPad

Mooi die iPad van de provincie

Meest gemelde incident in 2018:

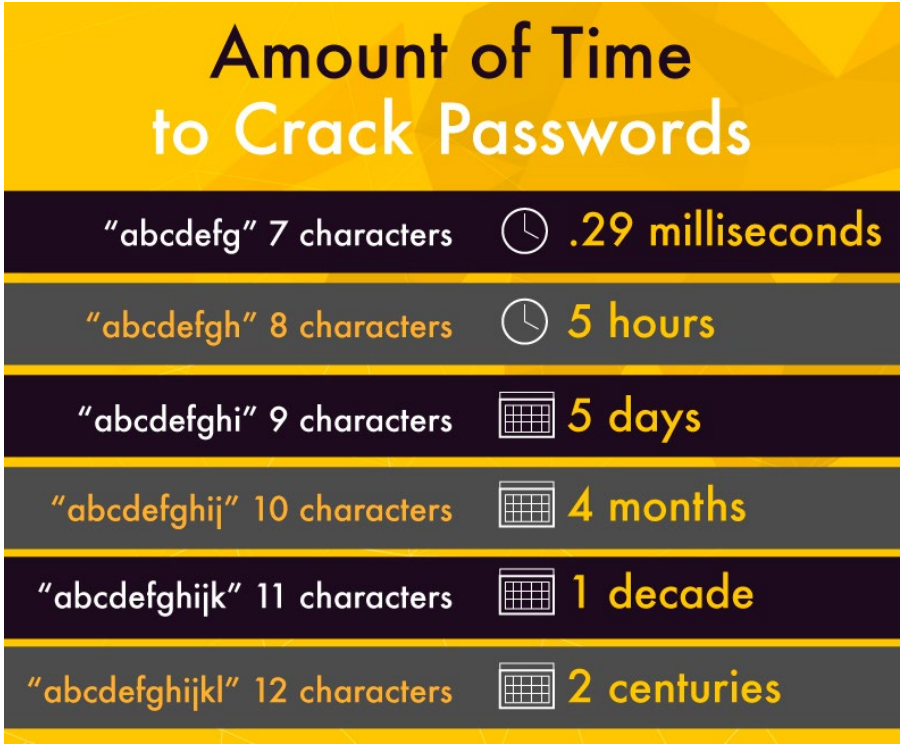
“Ik weet mijn wachtwoord niet meer”

“Mijn wachtwoord is geblokkeerd”

Wat is JE wachtwoord?

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123
16. football
17. 123123
18. monkey
19. 654321
20. !@#$%^&*
21. charlie
22. aa123456
23. donald
24. password1
25. qwerty123

Vervelende wachtwoorden



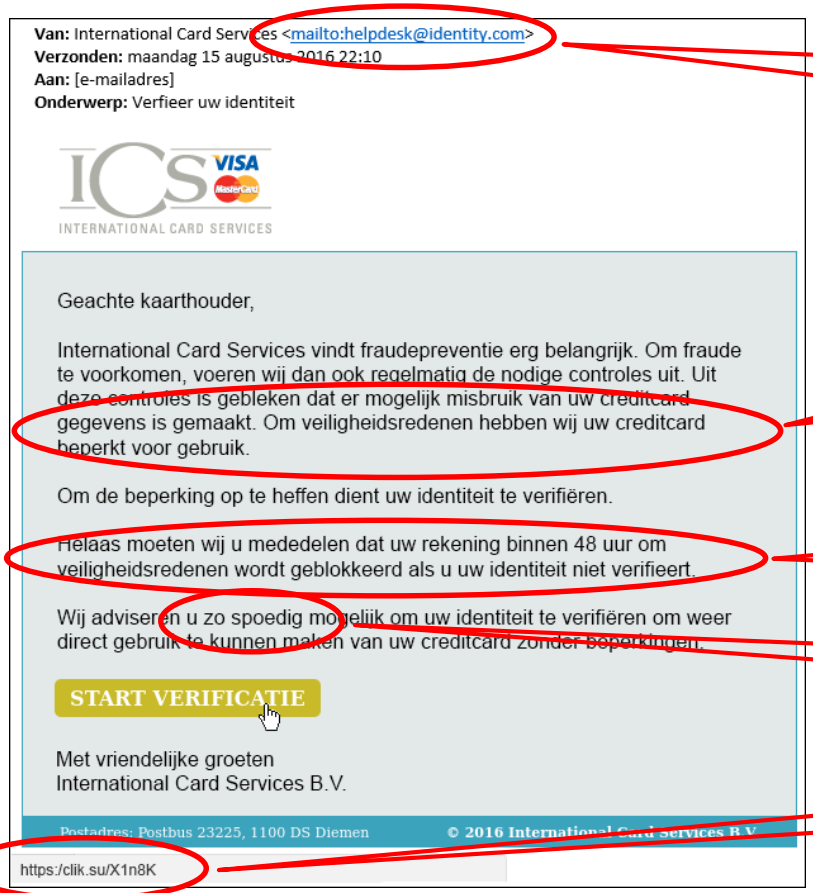
Bron: https://www.betterbuys.com/estimating-password-cracking-times/

- ✓ Paswoordzin
- ✓ Niet logisch voor een ander
- ✓ Bestaat uit:
  - ✓ Hoofdletters
  - ✓ Kleine letters
  - ✓ Cijfers
  - ✓ Speciale karakters
- ✓ B[illegible]

Geheim…
Niet delen!!!

Mailen met …@provincie-utrecht.nl

Mailen met …@provincie-utrecht.nl



Van: International Card Services <mailto:helpdesk@identity.com>
Verzonden: maandag 15 augustus 2016 22:10
Aan: [e-mailadres]
Onderwerp: Verfieer uw identiteit

ICS VISA MasterCard
INTERNATIONAL CARD SERVICES

Geachte kaarthouder,

International Card Services vindt fraudepreventie erg belangrijk. Om fraude te voorkomen, voeren wij dan ook regelmatig de nodige controles uit. Uit deze controles is gebleken dat er mogelijk misbruik van uw creditcard-gegevens is gemaakt. Om veiligheidsredenen hebben wij uw creditcard beperkt voor gebruik.

Om de beperking op te heffen dient uw identiteit te verifiëren.

Helaas moeten wij u mededelen dat uw rekening binnen 48 uur om veiligheidsredenen wordt geblokkeerd als u uw identiteit niet verifieert.

Wij adviseren u zo spoedig mogelijk om uw identiteit te verifiëren om weer direct gebruik te kunnen maken van uw creditcard zonder beperkingen.

START VERIFICATIE

Met vriendelijke groeten
International Card Services B.V.

Postadres: Postbus 23225, 1100 DS Diemen © 2016 International Card Services B.V.

https://clik.su/X1n8K

Kent u dit Email adres?

Oh nee, U heeft een probleem

U wordt gestraft

Snel handelen, urgent

URL is niet herkenbaar

Mailen met …@provincie-utrecht.nl

- ✓ Bedoeld voor provincie communicatie
- ✓ Niet bedoeld voor versturen vertrouwelijke stukken
- ✓ Alle mails worden gefilterd op malware en phishing, echter geen 100% zekerheid
- ✓ Automatisch doorsturen mail niet mogelijk
- ✓ Verdachtemail@provincie-utrecht.nl

Spreken in het openbaar

- ✓ Wees bewust van je omgeving
- ✓ Zoek een rustige plek
- ✓ Spreek je collega aan

Hacken zonder IT kennis: CEO fraude

10 november 2018 11:36
Laatste update: 10 november 2018 11:46

322

De Nederlandse directie van bioscoopketen Pathé is eerder dit jaar slachtoffer geworden van fraudeurs. In totaal is er ruim 19 miljoen euro buitgemaakt, blijkt uit een vonnis van de Amsterdamse rechtbank dat deze week werd gepubliceerd.

Tot slot

Bedankt voor je aandacht

Voor vragen en opmerkingen:
IB@provincie-utrecht.nl
Privacy@provincie-utrecht.nl