Ictoria

IT Beveiliging

Ictoria

Inhoud

- Phishing
- Vastleggen van gegevens
- Delen van gegevens
- Fysieke toegang
- Wachtwoorden
- Mail gebruik
- Internet gebruik
- Quiz

Ictoria

Phishing

- Wat is Phishing?
- Voorkomen van ..

Ictoria

“Phishing is een vorm van internet oplichting en fraude”

Phishing

Voorkomen door:

1. Neem IT maatregelen ter voorkoming
2. Gebruik goede spamfilter
3. Zorg voor bewustwording
4. Controleer de afzender bij mail
5. Controleer de link voor je ergens op klikt
6. Controleer de URL van de site
7. Wees alert op aanvallen
8. Zorg voor een veilige meld omgeving

En meld dit dan ook !!

- phishing via mail
- …. via telefoon
- …. via WhatsApp
- …. via post
- …. via website (marktplaats)
- …. via social media
- Spearphishing
- Catphishing
- Spoofing

\"Phishing is de eenvoudigste soort cyberaanval en tegelijk de meest gevaarlijke en effectieve\".

Ictoria

Omgaan met gegevens

- Vastlegging
- Klantgegevens
- Persoonlijke gegevens

Ictoria

Gegevens

- Klantcontact -> Wat schrijf je op, wat niet?
- Vastleggen van gegevens van de collega
- Info op tafel of toegankelijk?
  - Zichtbaar op tafel
  - Beschikbaar via toegang tot mappen
  - Scherm locken (Windows toets + L) !
- Blaadjes met wachtwoorden
- Delen van klantgegevens
  - Verwijs naar de voorwaarden
  - Handel altijd uit AVG gedachte
- Delen van je eigen gegevens?
  - Gebruik je zakelijke email alleen als nodig
  - Alleen aan bevoegde collega's
  - Vraag wat er met je gegevens gebeurt

Ictoria

1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data Protection Impact Assesment
5. Privacy by design & privacy by default
6. Functionaris Gegevensbescherming
7. Meldplicht datalekken
8. Bewerkersovereenkomsten
9. Leidende toezichthouder bepalen
10. Toestemming

AUTORITEIT PERSOONSGEGEVENS

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/algemene-informatie-avg

https://www.kvk.nl/advies-en-informatie/avg/voldoen-aan-de-avg-algemene-verordening-gegevensbescherming/

Phishing

Ictoria

Wachtwoorden

- Complexiteit
- Opslaan van je wachtwoorden
- Verschillende wachtwoorden
- Websites / opslaan in browser
- 2FA of MFA
- WiFi

Ictoria

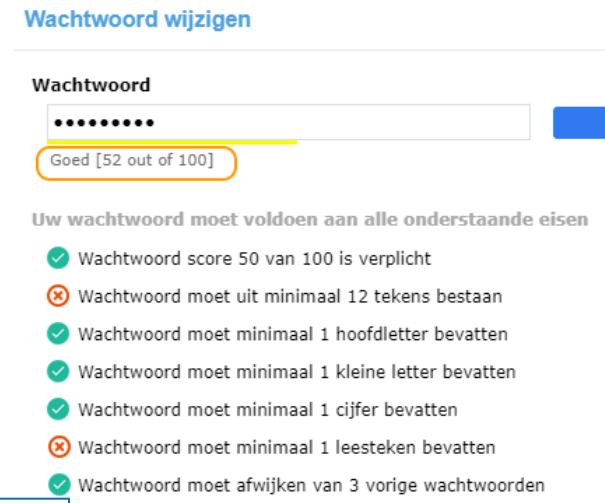
Wachtwoorden

1. Wachtwoord complexiteit

Regelmatig moet je ergens een wachtwoord voor opgeven. Dit kan voor een applicatie zijn, je computer, je mail of een website.

Wat kun je doen?

Maak lange wachtwoord zinnen, geen gebruik van namen van kinderen, bekende data of bekende teksten. Maak voor alles een apart wachtwoord, en houd de wachtwoorden niet bij op papier of in Word/Excel/Notepad/… maar gebruik van een wachtwoorden app.



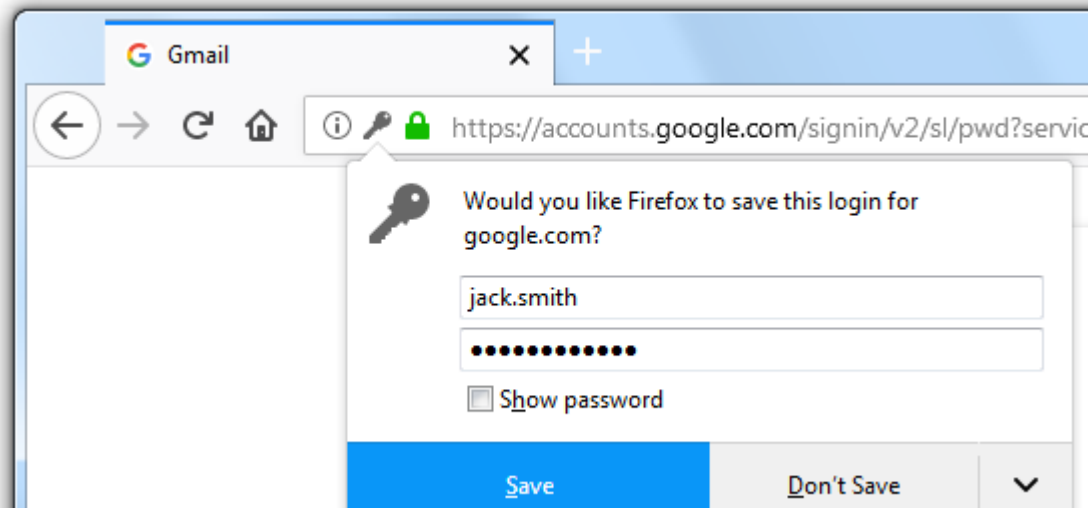
2. Wachtwoorden in browser

Als je een internet browser gebruikt krijg je regelmatig een vraag voor het opslaan van je wachtwoorden.

Wat kun je doen?

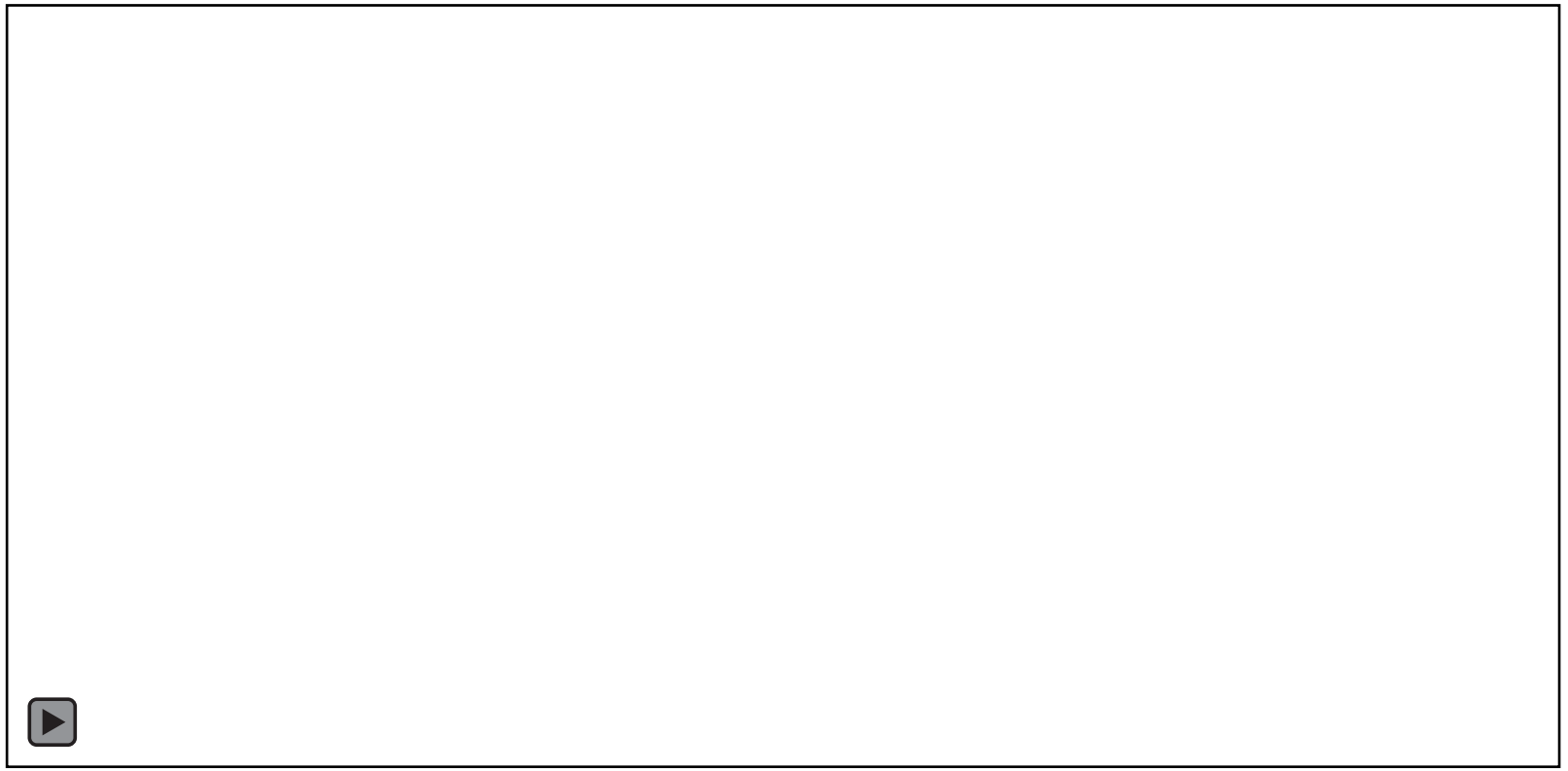
Maak gebruik van een wachtwoorden database /app. Laat deze de wachtwoorden invullen.

KeePass
Password Safe



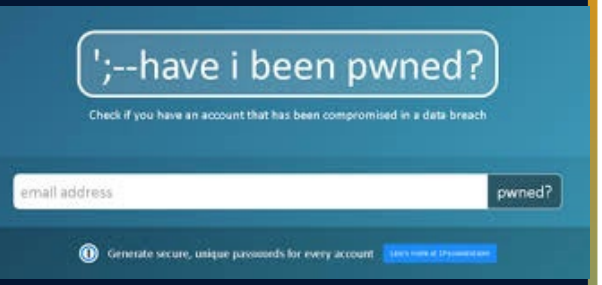
Ictoria

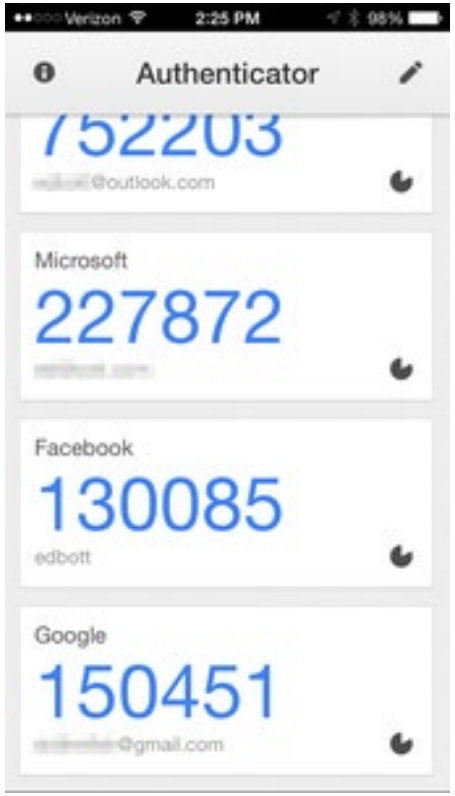
Wachtwoorden



Ictoria

Wachtwoorden





3. Maak gebruik van Multi Factor Authenticatie (MFA / 2FA)

Waar mogelijk, maak dan gebruik van meerdere authenticatie methoden.

Wat kun je doen?

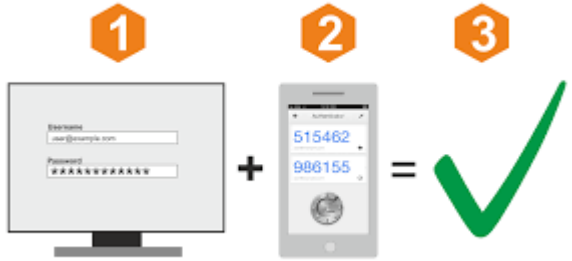
Gebruik daarvoor een app (denk aan Microsoft- of Google authenticator) of je mobiele nummer.

4. WiFi gebruik

Maak geen gebruik van gratis WiFi punten zoals MacDonalds of andere openbare plekken.

Wat kun je doen?

Gebruik in geval van je 4G -> Personal Hotspot. Maak gebruik van een VPN verbinding.



Ictoria

E-Mail

- Bijlagen
- Linkjes in de e-mail
- “Stevige boodschap”
- Aanhef van de mail
- Taalgebruik

Ictoria

E-mail

1. Pas op met het openen bijlagen

Regelmatig wordt in een “phishing” mail verwezen naar een bijlage.
Bijvoorbeeld voor een factuur of informatie rondom pakketleveringen.
Deze bijlagen bevatten vaak schadelijke software die op de computer wordt geïnstalleerd en bijvoorbeeld je bestanden kunnen versleutelen.

Wat kun je doen?

Open een bijlage alleen als je zeker weet dat de e-mail van een vertrouwde afzender komt. Wees extra voorzichtig met het openen van ZIP-, PDF- en Officebestanden.

2. Pas op met klikken op links in e-mails

De kans is namelijk aanwezig dat je wordt doorverwezen naar een valse website. Ook is het mogelijk dat je inloggegevens bekend worden bij de zender van de mail.

Wat kun je doen?

Je kunt met je muis over een link in de mail gaan (zonder erop te klikken!). Het webadres waar de link naar verwijst, verschijnt dan in beeld. Controleer of deze link naar een website gaat die overeen komt met de afzender. Vaak worden “aangepaste” versies van bekende websites gebruikt (goog.le.com).
Open deze link dan niet!

3. Wees alert op berichten met een ‘stevige boodschap’

Regelmatig bevat een phishing mail een ‘stevige boodschap’ om je te overtuigen. Bijvoorbeeld dat je pinpas wordt geblokkeerd of dat je bent vergeten om een factuur te betalen.

Wat kun je doen?

Een bank benadert je nooit direct op deze manier. Betreft het een andere instelling, ga dan na of je de afzender herkent. Check in je administratie recente bestellingen of facturen en bepaal op deze manier de betrouwbaarheid.

Ictoria

4. Let goed op de aanhef van de mail

Bij phishing mail wordt vaak gebruik gemaakt van een algemene aanhef zoals “Geachte heer/mevrouw”. Soms zie je ook dat men een aanhef gebruikt die niet gebruikelijk is. Bijvoorbeeld “Geachte J. Jansen”.

Wat kun je doen?

Wanneer organisaties je persoonlijk aanschrijven, zullen zij ook een persoonlijke aanhef gebruiken in e-mailberichten. Bijvoorbeeld: “Geachte heer Jansen”.

5. Wees extra alert op taalgebruik

Phishing mail bevat vaak tekst die door een vertaalcomputer is gehaald. Dat levert vaak vreemde zinsconstructies en taalfouten op. Inconsequent hoofdlettergebruik en rare interpunctie zijn ook geen goed teken. E-mails van echte bedrijven en officiële instanties zijn doorgaans een stuk netter geschreven.

6. Let op bijlagen!

Phishing mail bevatten regelmatig een bijlage. Deze bijlage kunnen virussen bevatten of code aanroepen van bijvoorbeeld een lek in de beveiliging.

Wat kun je doen?

Klik niet zomaar op een bijlage in een mail van een onbekende afzender.

Internet

- Browser gebruik
- Let op het sleuteltje
- Melding van Firewall/browser of Antivirus
- Websites wat wel of niet?

Ictoria

Internet

1. Gebruik een veilige browser (geen internet explorer)

De internet browser leest code van een website om dit te vertalen naar iets wat uitgevoerd wordt. Dit kan de code voor een website zijn maar ook om bijvoorbeeld iets te installeren of om code van jouw computer aan te roepen. Denk daarbij aan veiligheidslekken van het besturingssysteem of van een bepaalde applicatie zoals Adobe Reader.

Wat kun je doen?

Gebruik een veilige internet browser (Chrome/Firefox). Installeer (of laat dit doen) altijd updates van het besturingssysteem of van de applicaties (dus ook de browser). Gebruik ook plugins in browser voor veiliger internet gebruik.

2. Let op het sleuteltje en op de URL

Elke zichzelf respecterende website maakt gebruik van veilige communicatie. Dit wordt uitgebeeld door het sleuteltje en is leesbaar als httpS://www.....

Wat kun je doen?

Controleer altijd of je op de juiste website zit en of het sleuteltje wordt getoond. Bij twijfel… NIET DOEN!

Mede door gebruik van een goede browser wordt je gewaarschuwd voor louche sites.

Ictoria

3. Melding van Firewall (Windows Defender), browser of Antivirus

Er kan in een aantal gevallen een melding verschijnen van de firewall software, de browser zelf of het Antivirus programma dat een website niet veilig is, er een probleem is met de website of dat een site niet veilig zou zijn.

Wat kun je doen?

Als een dergelijk bericht getoond wordt dan niet verder gaan! Kijk op basis van het type melding en de URL wat er mis kan zijn zoals een typefout of iets dergelijks.

4. Websites: Wat wel of wat niet?

Let op als je websites bezoekt dat je alleen websites bezoekt die “dubieus” van aard zijn. Je hebt zelf wel een beeld wat gepast is, wat klopt en wat niet kan. Zie ook de medewerkersgids voor advies. Bij twijfel NIET DOEN !!

Melden !!

-Lijst frauduleuze handelaren en websites:
https://www.politie.nl/aangifte-of-melding-doen/bekende-malafide-handels...

-Controle of uw email account en wachtwoord mogelijk gehackt zijn

https://Haveibeenpwned.com

-Overzicht van storingen bij providers:
www.Allestoringen.nl

-Informatie over ransomware:
www.Nomoreransom.org

-Fraude Helpdesk
www.fraudehelpdesk.nl

https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en-antwoord/waar-kan-ik-cybercrime-melden

https://www.rijksoverheid.nl/wetten-en-regelingen/productbeschrijvingen/aangifte-doen-bij-politie of via 0800-700 (meld misdaad anoniem) of via politiebureau.

Ictoria

Quiz 1

1. Wat is een beter wachtwoord?

A. : DitismijnPowerPointPresentatieenikvindhetmooi#IctoriaRulez!!

B. : CE@dEfe22ea@#!

2. Je ontvangt een SMS van de ING met de vraag of je wil bellen met de ING helpdesk

A. : Je stuurt een SMS terug met de vraag om bevestiging

B. : Je belt naar het opgegeven nummer en vraagt aan de medewerker van de helpdesk of het inderdaad de ING is.

C. : Je belt het algemene nummer en vraagt wie er een SMS heeft gestuurd?

D. : Je meld het SMS-je bij de Fraude Helpdesk

E. : Je doet helemaal niets

3. Je krijgt het CV van een vriend(in) met het verzoek om deze bij Ictoria onder de aandacht te brengen. Yasemin werkt die dag niet en Nadia verwijst naar Yasemin. Wat doe je?

A. : Je legt het CV omgekeerd op het bureau van Yasemin

B. : Je legt het CV dichtgevouwen onder het toetsenbord van Yasemin

C. : Je legt het CV op het bureau van Yasemin.

D. : Je geeft het persoonlijk aan Yasemin als ze er weer is.

Ictoria

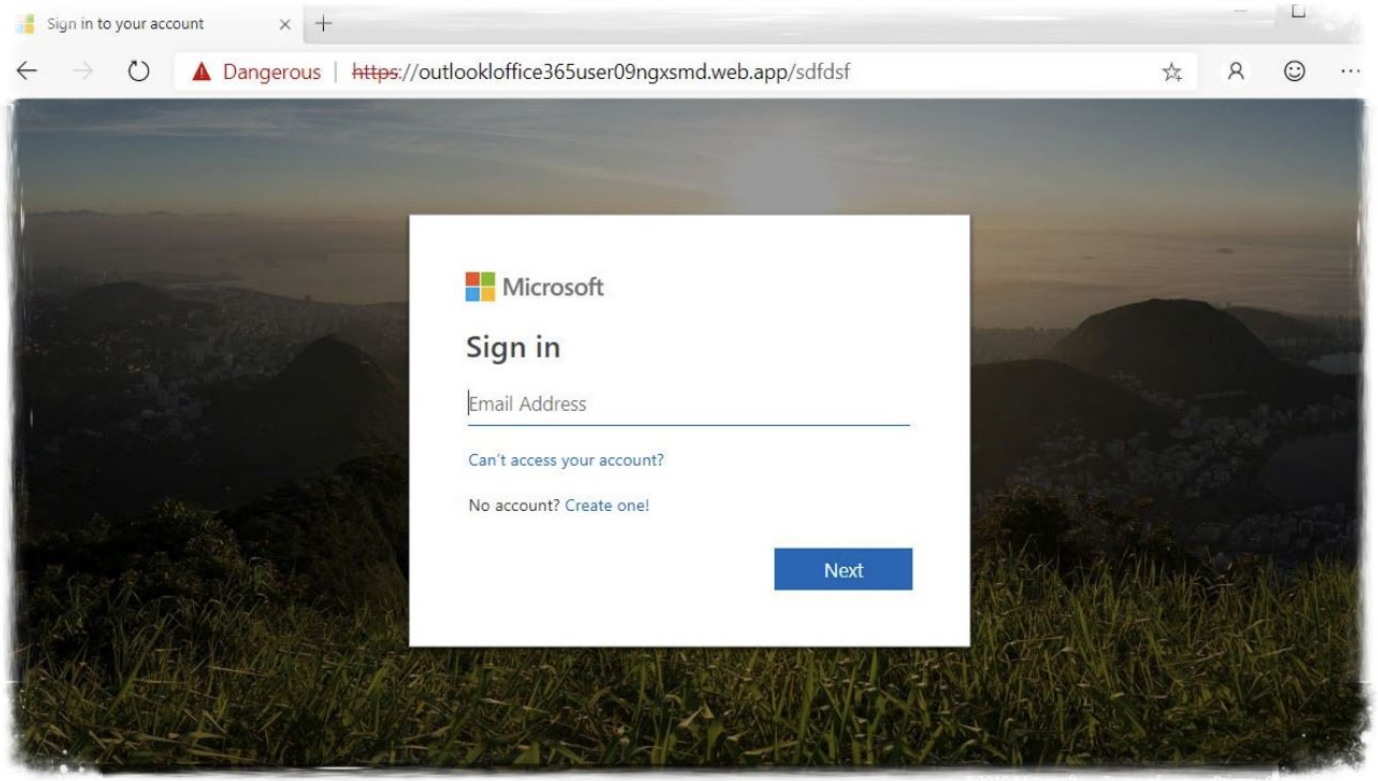
Quiz 2

4. Je klikt op een linkje op een site met tips over Outlook voor Office365 en gaat naar de site om in te loggen voor Office365 (zie onderstaande scherm).

A. : Je logt netjes in met je username en wachtwoord

B. : Je drukt op <CTRL> + <F5> om de pagina te verversen zodat je weet dat de pagina goed is.

C. : Je gaat alsnog naar de Ictoria start pagina om dan opnieuw op het mail icon



Ictoria

Quiz 3

5. Is het mogelijk dat iemand een mail stuurt vanaf jouw email adres?

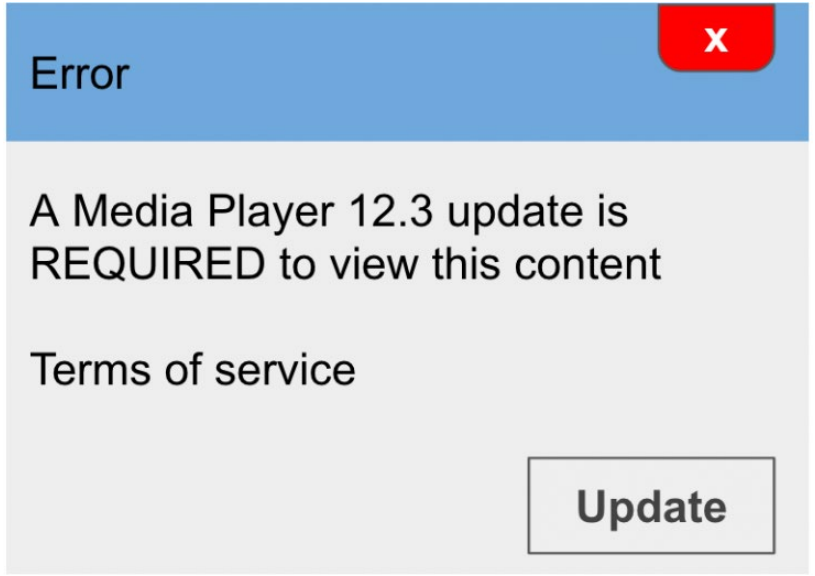
A. : Nee kan niet als ze mijn wachtwoord niet hebben
B. : Ja, dat kan.
C. : Geen idee, dat zal toch niet?

6. Je krijgt onderstaande melding op een website. Wat doe je?

A. : Update
B. : Negeren
C. : Even vragen bij de helpdesk

7. AVG staat voor?

8. GDPR staat voor?



Ictoria

6. Je wordt gebeld door de Microsoft met de mededeling dat iemand probeert in te loggen met je account. Ze vragen ter bevestiging je login naam of emailadres. Wat doe je?

A. : Geeft het emailadres of je login naam en vraagt wat je moet doen
B. : Belt terug naar het nummer om te controleren of het nummer klopt
C. : Doet niets en bedankt ze voor het melden
D. : Veranderd je wachtwoord in overleg met Microsoft.

7. Een klant stuurt je een email met daarin zijn login gegevens voor het website beheer. Wat doe je met die gegevens?

A. : Mail verwijderen
B. : Mail printen en aan bij de verantwoordelijke collega op zijn bureau leggen
C. : Mail doorsturen naar alle collega's binnen Ictoria zodat de verantwoordelijke dit kan oppakken
D. : Vastleggen in een speciale tool

8. Een medewerker van het COB belt dat er ingelogd moet worden op de COB website. De medewerker zegt dat je hun het wachtwoord niet moet geven maar alleen moet inloggen op een site. Wat doe je?

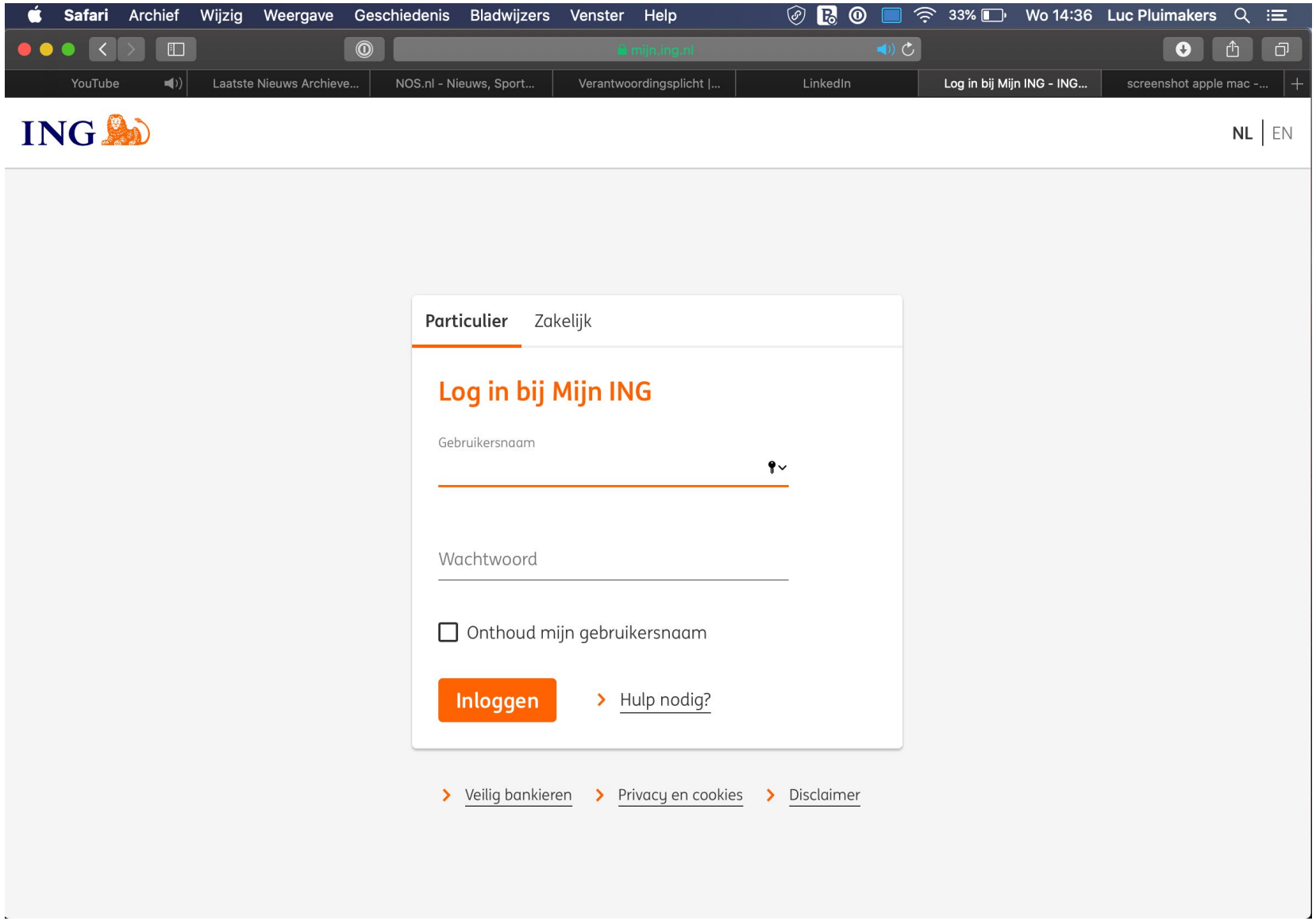
A. : Geeft het wachtwoord gewoon
B. : Belt terug naar het nummer om te controleren of het nummer klopt
C. : Doet niets en bedankt ze voor het melden
D. : Je gaat naar de aangegeven website en logt daar in zodat je niet het wachtwoord verklapt aan
de medewerker

Quiz 4

Ictoria

Quiz 5

9. Wat klopt er niet?



Ictoria

DANK!

Herbert van den Heuvel

+31 (0)85 876 9214
+31 (0)6 51856151

www.ictoria.nl
herbert.van.den.heuvel@ictoria.nl