# Cyberlunch Digitaal Veilig Ondernemen

Restaurant Soesterduinen

BMO SOEST

Gemeente Soest

POLITIE

PVO Midden-Nederland

# Welkom!

- **Karin Scholten:** Wethouder Economische zaken gemeente Soest
- **Merel Hurenkamp:** 5 basisprincipes van digitaal veilig ondernemen
- **Bastiaan Ramp:** Wat doet de politie?
- Samenvatting en to do’s

# Karin Scholten, Wethouder Economische Zaken gemeente Soest

Gemeente
Soest

# 5 basisprincipes van digitaal veilig ondernemen

Merel Hurenkamp

8 juni 2023

LEGIAN

PVO / Midden-Nederland

# Veiligheid

**1:8000**

De kans op brand
in je bedrijf

**1:250**

De kans op inbraak
in je bedrijf

**1:5**

De kans op
een cyberaanval

# Ik hoor jullie denken…

- Een cyberaanval overkomt mij niet;
- Mijn IT-leverancier regelt dat voor me;
- Wij zijn te klein;
- Ik weet dat ik er iets mee moet, maar waar moet ik beginnen?
- Wat moeten criminelen met onze gegevens?

**Jij bent niet de enige die dat denkt…**

# Bakker logistiek

- Verantwoordelijk voor **25%** van de toelevering van levensmiddelen in Nederland
- De leverancier van Albert Heijn

## April 2021: ‘Kaas-hack’

- Ransomware aanval: de levering vanuit 3 grote magazijnen werd stilgelegd
- 250 vrachtwagens konden niet weg
- Alle systemen lagen plat
- Beveiligingslek in Microsoft Exchange

# Vertrouw niet zomaar op software en/of je IT-leverancier.

PVO / Midden-Nederland

# Bakker Ineke

- Kleine bakkerij in Noord-Brabant
- Allergievriendelijke broden
- 50 klanten
- Bakfiets

## Mail van de belastingdienst

- Al haar gegevens kwijt
- Bijzondere persoonsgegevens
- Boete van autoriteit persoonsgegevens
- Failliet

# Jouw gegevens zijn belangrijk voor jou en je bedrijfsvoering.

## 60% van de mkb’ers gaat na een hack binnen 6 maanden failliet.

PVO / Midden-Nederland

# Iedereen kan slachtoffer worden van cybercriminaliteit!

## 5 basisprincipes van veilig digitaal ondernemen

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en malware

# 1. Inventariseer je kwetsbaarheden

## Algemeen belang

- Inventarisatie kroonjuwelen
- Wie is er in jouw organisatie verantwoordelijk voor back-ups? Staat dat ergens zwart op wit?

**To do: Maak een risicoanalyse of inventarisatie. Bespreek verantwoordelijkheden en leg afspraken vast.**

# 1. Inventariseer je kwetsbaarheden

## Help! Ik ben gehackt!

- Wat nu?
- Hebben jullie een incident responsplan? Digitaal of fysiek?
- En back-ups? Doen die het ook?

## “Autoverhuurbedrijf dagen lang stil door hack: incident responsplan ook versleuteld”

**To do: Maak een calamiteitenplan en plan voor back-ups (patchbeleid). Bewaar deze goed!**

# 2. Kies veilige instellingen

## Instellingen

- Controleer de instellingen: welke apparaten zijn gekoppeld aan het internet? Is er overal sprake van MFA?
- Maak gebruik van een firewall
- Zorg voor voldoende loginformatie

## De zwakste schakel bepaalt de sterkte van de keten

# 2. Kies veilige instellingen

## Alles wat met het internet verbonden staat is te hacken

- Werken jouw medewerkers hybride?
- Hoe is het gesteld met de WiFi thuis?
- BYOD

- Welke apparaten op kantoor staan verbonden met het internet?

## “23 jarige jongeman uit Nederland hackt printers van universiteit in Amerika”

# 2. Kies veilige instellingen

## Digitale poortwachter

- Wat is een firewall?
- Wat is loginformatie?

- Voorkomt ongeautoriseerde toegang
- Detecteert ongebruikelijke activiteit

**To do: Vraag je systeembeheerder of IT-leverancier hoe en waar jouw loginformatie is opgeslagen? En of je een firewall hebt.**

# 3. Voer updates uit

## Stop met wachten tot vrijdagmiddag

- Wie stelt wel eens een update uit?

### Bij updates lossen systemen kwetsbaarheden op in de software: ze verbeteren de sloten van openstaande deuren

- Zodra een update uitkomt weten ook criminelen van de slechte sloten
- De tijd tussen de slechte sloten en goede sloten moet zo beperkt mogelijk blijven

# 3. Voer updates uit

## Installeer ook de patches!

- Patches zijn letterlijk pleisters, kleine tussentijdse updates die worden gebruikt om kleine fouten te verbeteren
- Zijn de updates centraal geregeld of is de medewerker zelf verantwoordelijk?

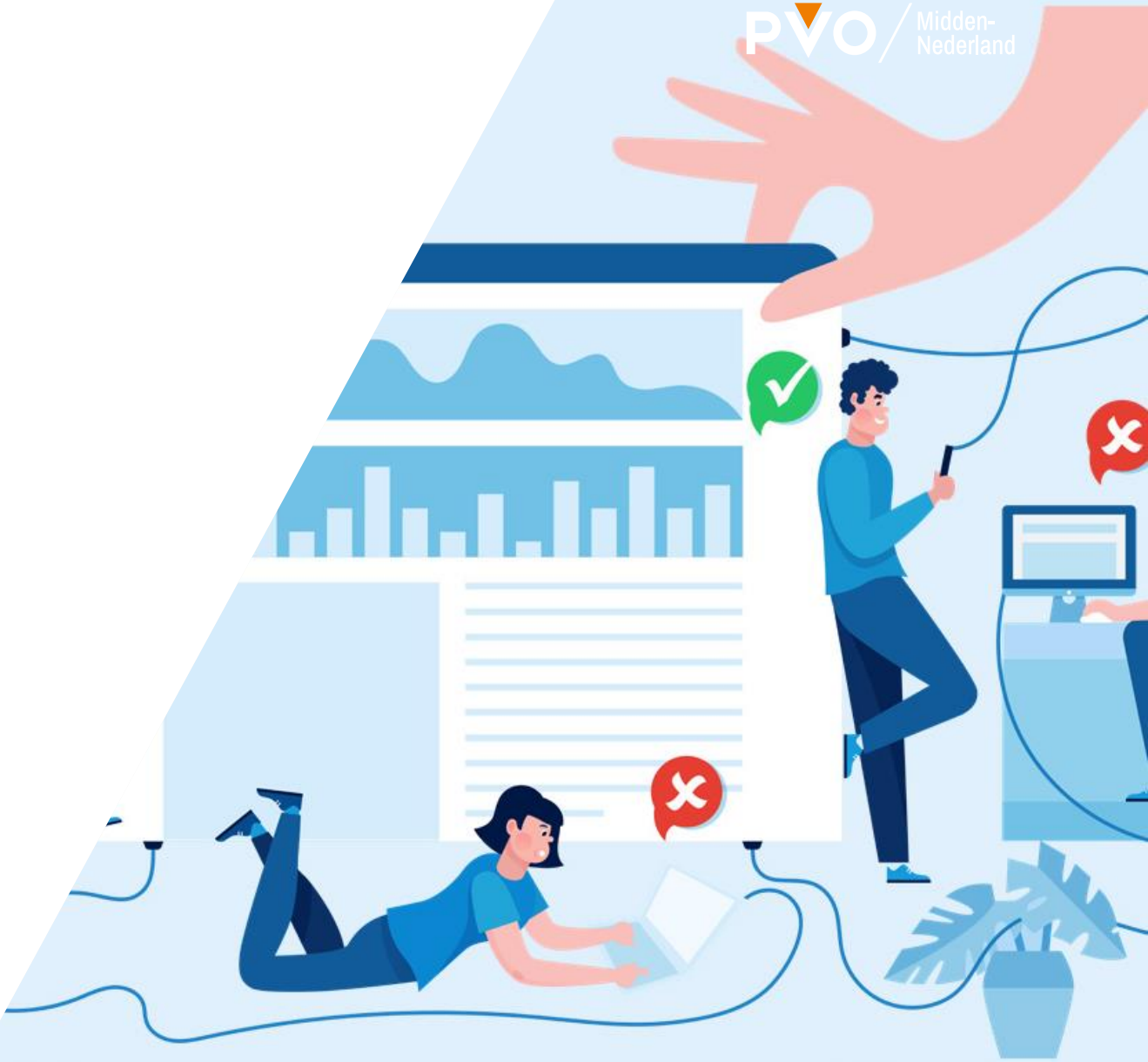
**To do: voer updates direct uit, zet automatisch updaten aan en bespreek de afspraken over updaten intern.**

# 4. Beperk toegang

## “U heeft geen toegangsrechten voor deze pagina”

- Hebben al jouw medewerkers dezelfde toegangsrechten?
- Wees kritisch op wie je welke rechten geeft
- Vertrouwen

- Wat is het beleid als iemand stopt met werken?



# 4. Beperk toegang

## “Welkom123”

- Hoeveel tekens is jullie wachtwoord?
- MFA

- Dictionary attack, brute force, social engineering
- Zorg voor minimaal 18 tekens: wachtwoordzinnen
- Gebruik niet dezelfde wachtwoorden (passwordmanager)

**Cybercriminelen zullen in geen 100 jaar mijn wachtwoord hacken!**

# 4. Beperk toegang

**To do:**

- inventariseer de toegangsrechten van je medewerkers en wees kritisch;
- wat doe je als een medewerker uit dienst gaat (leg dit vast);
- zorg voor goede wachtwoorden;
- zorg voor MFA en maak hierover intern afspraken;
- voorkom tailgating en wees je bewust wie zich in jouw pand bevindt;
- zorg voor automatische vergrendeling van devices.

# 5. Voorkom virussen en andere malware

## Vormen

- **Virussen**
  - Trojan
  - Worm
- **Malware**
  - Ransomware

# 5. Voorkom virussen en andere malware

## Bescherm je tegen virussen

- **Gedrag:** human factor en vergroot bewustwording
- **Techniek:** antivirusprogramma
- **Organisatie:** beperk installatiemogelijkheden apps en denk na over processen

**To do: biedt cyberawareness aan voor je medewerkers, beperk installatiemogelijkheid van apps, inventariseer of en welk antivirusprogramma je hebt.**

# Cyberawareness

## 1 klik verwijderd van een cyberaanval

- Train / test jezelf en je personeel
- Neem het op als terugkerend onderwerp in interne vergaderingen
- Neem het op in onboardingsproces
- Pas kracht van herhaling toe

www.betalen.rabobank.nl

www.rabobank.betalen.nl

# Iedereen kan slachtoffer worden van cybercriminaliteit!

## 5 basisprincipes van veilig digitaal ondernemen

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en malware

# “Wat doet de politie”

Wat mag u verwachten?

« waakzaam en dienstbaar »

# Introductie:

Bastiaan Ramp

Operationeel Specialist

Digitale Opsporing (Recherche)

# Waarheen?

# Hoe alert bent u?

## Het kan iedereen overkomen.

# Wat ‘ziet’ de politie?

*“In 2022 kwam 33% van de mkb’ers in aanraking met virussen en phishing,*

*13% van de organisaties met ransomware.”*

**Aangiftebereidheid na slachtofferschap;**
**14% van de mkb’ers.**

*“De ondernemers willen zo snel mogelijk door.”*

# Wat ‘ziet’ de politie?

*Cybercrime & gedigitaliseerde criminaliteit*
***neemt toe!***


**Dit is een prioriteit voor de politie.**

# Wat ziet de politie?

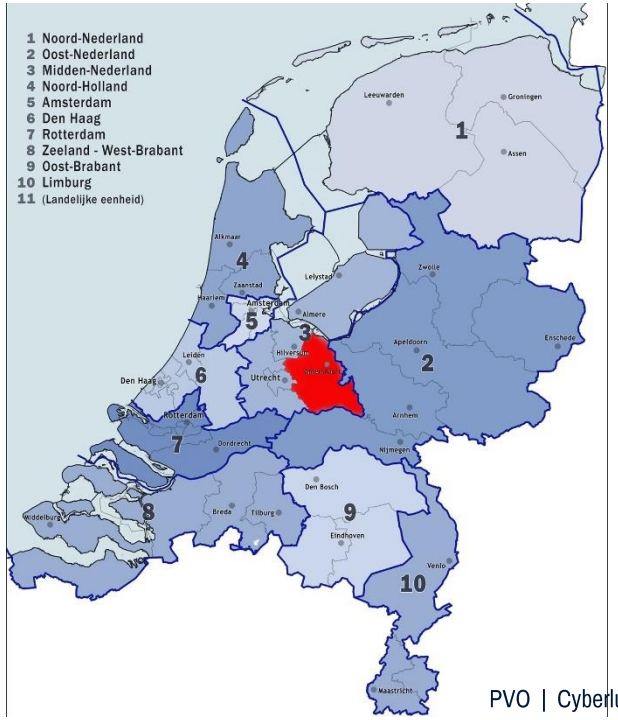
## Niet hetzelfde!

Landelijk in 2022 ziet de politie

**170** aangiftes ransomware.


District Oost-Utrecht in 2022:

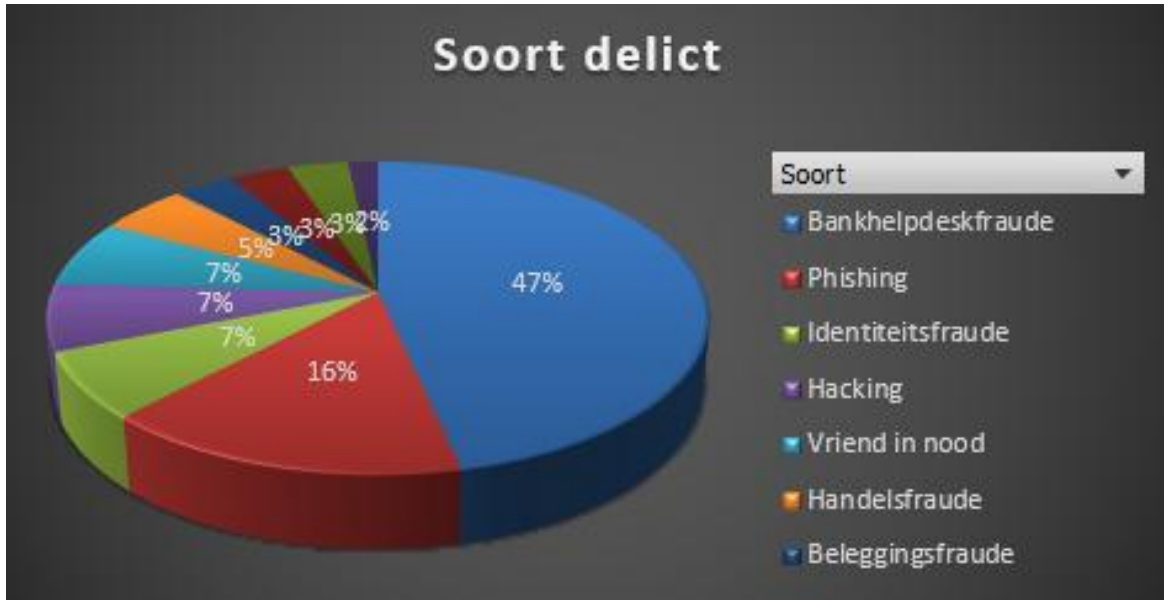
**2.500** cyber/digi aangiftes



# Wat ziet de politie?

## Niet hetzelfde!

### Beeld in Oost-Utrecht *(feb 2023)*




| Soort delict | Aantal |
|---|---|
| Bankhelpdeskfraude | 27 |
| Phishing | 9 |
| Identiteitsfraude | 4 |
| Hacking | 4 |
| Vriend in nood | 4 |
| Handelsfraude | 3 |
| Beleggingsfraude | 2 |
| Sextortion | 2 |
| Identiteitsfraude/CEO | 2 |
| Factuur fraude/CEO fraude | 1 |
| Eindtotaal | 58 |

# Aangiftebereidheid na slachtofferschap

| Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie? | MKB N= 488 | Grootbedrijf N= 669 |
|---|---|---|
| Mails ontvangen met poging tot phishing | 20% | 25% |
| Benaderd op sociale media met een vraag om een onbekende link aan te klikken | 4% | 1% |
| Ransomeware | 1% | 0,4% |

**cijfers gebaseerd op eindgebruikers.*

## Schaamte bij medewerkers

Als er dan een aanval optreedt, wil je als bedrijf hier natuurlijk zo goed mogelijk mee omgaa
de hoogte bent van eventuele dreigingen, bijvoorbeeld wanneer een werknemer op een ph
gedownload. Helaas melden werknemers dit niet altijd, met name doordat zij zich schamen
zich te schamen als ze op een link in een phishing e-mail zouden klikken. 12% van de medev
schaamte bovengenoemde voorvallen niet zouden melden. Dit is een zorgelijke bevinding a
door het gedrag van mensen vaak weinig aandacht krijgt bij cybersecurity. Zorg er daarom
over gecommuniceerd kan worden.

| Wat zijn de belangrijkste redenen om geen aangifte of melding te doen? | Medewerkers N= 1166 |
|---|---|
| Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen | 62% |
| Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor ook andere computers binnen mijn bedrijf besmet (kunnen) raken dan vertel ik uit schaamte niet aan anderen wat ik heb gedaan | 12% |

# Slachtoffer en nu?

## Aangifte of melding?

# Slachtoffer en nu?

## Wat is belangrijk voor de politie.

(Digitale) Sporen:

- IP adressen
- URL's (webadressen & linkjes)
- Headers van e-mails
- Server logging

# Slachtoffer en nu?

## Het allerbelangrijkste = Tijd!

# Slachtoffer en nu?

## Phishing ontdekt!

# Wat kan de politie?

- Onderzoek doen,
- Informatie vorderen,
- Gegevensdragers uitlezen,
- Bureau Hengeveld /  Opsporing Verzocht,
- Netwerkpartners inzetten (fysiek & online),

# Behoefte en Verwachtingen

## Wat maakt Cybercrime voor u en de politie lastig?

# Behoefte en Verwachtingen

## Spelletje – Herken de boef:

VS

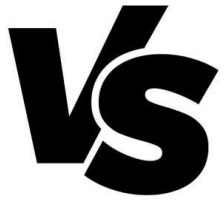
# Behoefte en Verwachtingen

## Spelletje – Herken de boef:

VS

# Behoefte en Verwachtingen

## Spelletje – Herken de boef:

185.12.65.44  185.12.65.46

# Wat beperkt de politie?

- Vluchtigheid gegevens
- Verwerking van vorderingen (tijd)
- Grensoverschrijdend
- Digitale anonimisering
- Personele inrichting (capaciteit)

# Behoefte en Verwachtingen

## Als politie zijn we nog steeds gek op boeven vangen!

En daar hebben we jullie bij nodig.

# Enkele resultaten:

AD NIEUWS REGIO SPORT SHOW VIDEO FUN


▲ © ANP

## Man misbruikte WhatsApp voor ‘schaamteloze’ oplichting: 20 maanden cel geëist

**Een 22-jarige man uit Almere die in mei in Amersfoort werd opgepakt voor whatsappfraude, moet als het aan het Openbaar Ministerie ligt 20 maanden de gevangenis in. Ook eiste de officier van justitie vanmiddag dat hij zijn slachtoffers een schadevergoeding betaalt.**

Redactie Amersfoort 06-11-19, 14:29 **Laatste update:** 06-11-19, 18:12

De Almeerder maakte zeker negen slachtoffers. Hij wordt er onder andere van verdacht dat hij zich via WhatsApp voordeed als familielid of bekende van zijn slachtoffers, door hun foto’s van internet te halen. Vervolgens vroeg hij hen om een factuur te betalen. Het geld werd overgemaakt naar de rekening van een katvanger.

## Tiener uit Amersfoort opgepakt voor 1 cent betaalfraude

Laatst gewijzigd op: 09-07-2021 | 09:57

Amersfoort - Een 16-jarige verdachte uit Amersfoort heeft op slinkse wijze meerdere mensen opgelicht. Met behulp van frauduleuze betaalverzoeken maakte de jongen hen veel geld afhandig. Maandag 5 juli werd de verdachte hiervoor van zijn bed gelicht door de politie.



Helene de Groot. Geplaatst: 20 augustus 2020 om 13:22.

AMERSFOORT - Opnieuw heeft politie twee verdachten weten aan te houden in een groot onderzoek naar cybercrime. Het gaat om een 22-jarige man uit Nieuw-Buinen en een 33-jarige man uit Helmond.

Vooral veel ouderen waren de dupe van de oplichtingspraktijken. Ruim 200 slachtoffers hadden zich gemeld bij politie. Deze slachtoffers dachten dat door hun bank werden gebeld die hen adviseerde om geld over te maken naar een veilige rekening, omdat er bijvoorbeeld een hack zou dreigen. De oplichters konden via Teamviewer op de computer het slachtoffer meekijken bij het overmaken van het geld. In werkelijkheid werd het geld weggesluisd naar rekeningen van zogenoemde geldezels of katvangers. De gestolen bedragen varieerden van 10.000 tot 100.000 euro.

In dit onderzoek werd eerder op 18 mei een 21-jarige Amersfoorter en een 30-jarige Veendammer aangehouden. Op 27 mei een 23-jarige man uit Veendam en op 2 juni een 23-jarige man en een 25-jarige vrouw uit Hilversum aangehouden. Bij doorzoekingen werden bij hen grote geldbedragen, dure auto’s, merkkleding, telefoons en computers in beslag genomen. De

dS DE STENTOR

Weer Extra Familieberichten Achter de Schermen dS Werkt Kla

REGIO ALGEMEEN SPORT VIDEO OPINIE FUN

Regio wijzigen Zwolle Apeldoorn Deventer Zutphen Kampen Veluwe Achterhoe


▲ Foto ter illustratie van de mobiele applicatie van Marktplaats.nl ©ANP XTRA

## Kopstukken in Marktplaats-fraude aangehouden in Salland: ‘13-jarige bedreigd om bankpas van moeder af te geven’

**Vier mannen uit Raalte en Wijhe zijn afgelopen woensdag opgepakt door de recherche voor online fraude. De jonge mannen verdienden met ticketoplichting ruim 21.000 euro. Onder het mom van identiteitsfraude wonnen ze het vertrouwen van 58 slachtoffers, die tussen de 80 euro en 400 euro voor tickets betaalden.**

Jeroen Achtereekte 11-06-20, 16:35 **Laatste update:** 16:54 **Bron:** de Stentor

In een klein jaar tijd maakten de mannen slachtoffers in heel Nederland. Het gaat om twee mannen van 18 en één man van 19 uit Raalte en een man van 21 uit Wijhe. Zij worden

# Vragen?



www.veiligdigitaal.com

www.nomoreransom.org

Politie: 0900-8844

www.politie.nl

# Wat ga je morgenochtend doen?

- Plan een afspraak met je IT-leverancier
- Ga met je medewerkers in gesprek
- Kijk of er updates mogelijk zijn op jouw devices
- Zorg voor een wachtwoord of wachtzin van minimaal 18 tekens
- Check de websites op de hand-out voor tips, tricks en meer informatie

# Zijn er nog vragen?

- Bedankt voor jullie aanwezigheid!

Gemeente Soest

BMO SOEST

POLITIE

PVO Midden-Nederland