# Hoe overleef ik een hacker?

## 20 tips om mezelf en mijn organisatie veilig te maken

CAK

# Waarom deze handreiking?

Elke dag meldt de media wel een datalek of een phishing aanval. Gelukkig zijn er technische beveiligingsmiddelen zoals een firewall en kennen we procedures over het gebruik van wachtwoorden. Hiermee voelen we ons als organisatie en als medewerker veilig en beschermd.

Maar is dat echt zo? In dit gevoel van veilig en beschermd zijn schuilt ook een zwakte. Misschien voelen we ons door zulke maatregelen wel te goed beveiligd en zien we toch zaken over het hoofd. Goed met informatie omgaan komt aan op zelf kritisch kijken wat je beter kunt doen. In je dagelijkse routines sluipen slordigheden of doe je dingen zonder het risico goed in te schatten.

Met deze handreiking willen we je de weg wijzen naar een informatieveilige wereld. We geven je praktische tips voor op het werk en thuis. En we vragen je om je digitale veiligheid en je dagelijkse gedrag kritisch te bekijken. Samen maken we onze organisatie sterk en weerbaar.

# Inhoud

Informatiebeveiliging en privacy worden vaak in één adem genoemd. In onze organisaties gaat het over beide. Daarom maken we ons niet druk om de definities.

We nemen je mee op reis en starten met het inrichten van een gezonde basis. Zodra die staat, leren we je hoe je de grootste risico's kunt herkennen. Heb je alles onder knie, kijk dan bij de expert tips. Als laatste: wie kan jou helpen als het toch misgaat.

Dus:

# START met een goede basis



## Checklist

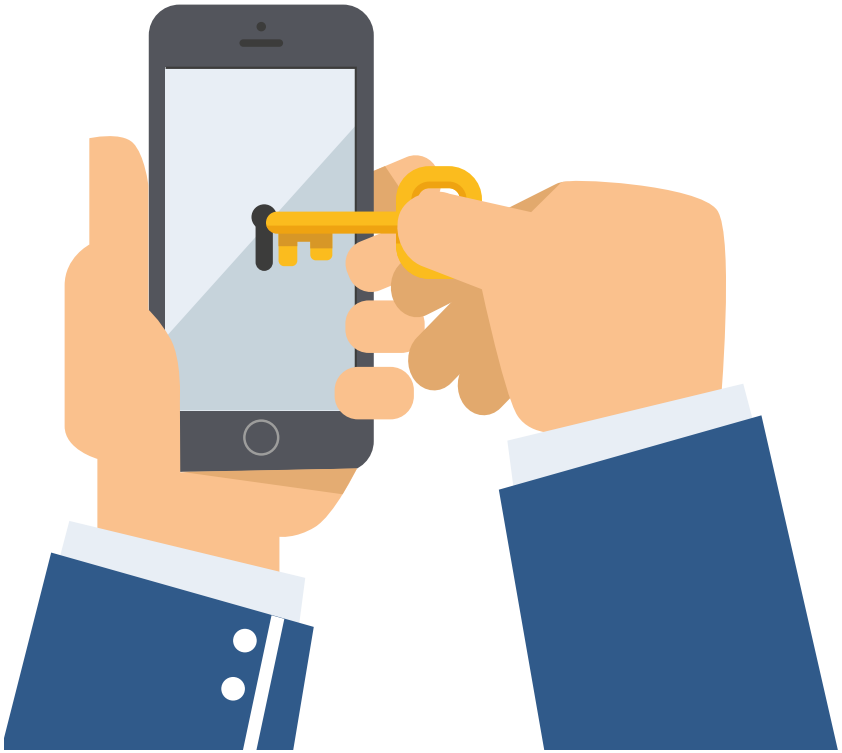
**Heb ik dit geregeld?**

- ☐ *Ik heb mijn smartphone beveiligd met een code*
- ☐ *Ik gebruik sterke wachtwoorden*
- ☐ *Ik ga zorgvuldig met gevoelige informatie om*

# Tip 1: Zet je mobieltje op slot

De meest gebruikte code is nog steeds 0000. Bedenk een sterkere combinatie en zet je mobieltje en tablet daarmee op slot.

Op je mobiele telefoon staat niet alleen veel informatie (namen en telefoonnummers), maar zonder code op je mobiel kan men ook makkelijker bij je bankrekening.





# Tip 2: Gebruik sterke wachtwoorden

Wachtwoorden... je hebt er zoveel en je moet ze allemaal onthouden. Daarom is het heel begrijpelijk dat je hiervoor bijvoorbeeld de naam van je kind plus zijn of haar geboortejaar gebruikt. Of de postcode van je huisadres. Helaas zijn dergelijke wachtwoorden makkelijk te achterhalen.

**Hoe doe je het goed?**

- **Neem voor alles een ander wachtwoord.**
  Voor je DigiD, social media, je werk en je privé e-mail.

- **Maak een sterk wachtwoord.**
  Maak een sterk wachtwoord.
  Gebruik minimaal 12 tekens, maar hoe langer hoe beter.
  Een sterk wachtwoord bestaat uit kleine letters, hoofdletters, getallen én speciale tekens.

Het enige wachtwoord dat je moet onthouden is het wachtwoord waarmee je inlogt op je laptop. Gebruik hiervoor een wachtwoordzin in plaats van een wachtwoord, bijvoorbeeld:

binnen oor Manage 15 stad

***Expert tip:*** *Te veel om te onthouden? Neem een wachtwoordmanager: met deze software hoef je maar één wachtwoord te onthouden, de rest regelt het programma.*
*Zie Tip 9 voor meer uitleg.*

# Veilig zakelijk bellen? Zo doe je dat:

Met het thuiswerken en hybride werken is de manier van communiceren en werken veranderd. Waar je voorheen collega's sprak in de gang, bij de koffieautomaat, aan het bureau of in een vergaderzaal heb je tegenwoordig veel vaker contact via telefoon, video vergaderen, e-mail of berichtendiensten. Dit heeft er ook voor gezorgd dat telefoongesprekken niet meer alleen in de werkkamer of achter het bureau plaatsvinden. Zo ga je misschien vaker op andere plaatsen werken of loop je buiten een rondje om (telefonisch) bij te praten.

### Weet wat je wanneer deelt

Het voeren van zakelijke gesprekken via de telefoon is niets nieuws, de locaties waar deze gesprekken plaatsvinden soms wel. Bespreek bijvoorbeeld nooit gevoelige of vertrouwelijke informatie wanneer je buiten aan het bellen bent, maar doe dit op kantoor of in een (afgesloten) ruimte waar je alleen bent.

Vermijd ook drukke plekken zoals de supermarkt, het terras, het station of de trein om werkinhoudelijke informatie te bespreken. Ondanks dat de informatie niet per se vertrouwelijk is, weet je niet wie er meeluistert. Als een omstander slechts een deel van het gesprek kan opvangen, kan dat stukje informatie uit zijn context getrokken worden met nadelige gevolgen. Word je gebeld op je werktelefoon terwijl je in een drukke omgeving bent, geef dan aan waar je je bevindt en beantwoord vragen alleen met ja/nee-antwoorden. Zo weet de beller ook wat hij of zij wel en niet kan bespreken. Melden dat je iets later terugbelt als je niet in de gelegenheid bent om rustig te bellen, is natuurlijk ook prima.

Kortom: Weet met wie je spreekt, waar je spreekt en waarover je spreekt.



# Tips

De volgende tips kunnen je helpen om niet alleen jezelf maar ook je collega's om bewust zakelijke telefoongesprekken te voeren:

**Als leidinggevende:**

- geef ik het goede voorbeeld bij het voeren van telefoongesprekken.
- spreek ik collega's aan wanneer ik merk dat de ander zich in een drukke omgeving bevindt tijdens het bellen.
- maak ik omgevingsbewustzijn tijdens het voeren van telefoongesprekken bespreekbaar in teamoverleggen door middel van voorbeelden of incidenten.

**Als medewerker:**

- ben ik mij bewust van mijn omgeving en bespreek ik vertrouwelijke informatie niet via de telefoon als ik niet alleen ben.
- geef ik het aan het begin van het telefoongesprek aan wanneer ik mij in de openbare ruimte bevind.
- ben ik mij bewust waar ik spreek, met wie ik spreek en waarover ik spreek en vraag ik of het gesprek uitgesteld kan worden totdat ik een vertrouwde omgeving ben.

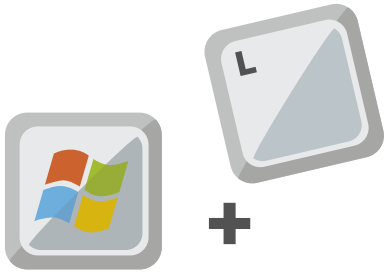
**Meer weten?**

Heb je nog vragen n.a.v. deze tekst?
Mail je vraag naar: tiso@hetcak.nl

# Tip 3: Maak afspraken over omgang met gevoelige informatie

Persoonsgegevens strooi je niet rond, maar ook informatie over je organisatie kan gevoelig zijn voor concurrentie of de pers. Spreek met elkaar af wat je bedoelt met gevoelige informatie en wat er van je verwacht wordt.

Tips om informatie veilig te verwerken.




**Houd je werkplek netjes**

- **Sluit je scherm af.**
  Even koffie halen?
  Sluit je scherm actief af:
  Windows L. Ook bij thuiswerken.

  N.B. vertrouw niet op de automatische vergrendeling van je scherm, want in de tussentijd kan iemand toch inloggen.

- **Ruim je prints op.**
  Hoe vaak vind jij printjes van anderen? Of originelen die zijn blijven liggen op de glasplaat? Ruim ze discreet op, want deze informatie is ook niet voor jou bedoeld. Ook bij thuiswerken.

- **Gebruik de versnipperaar en de speciale papierbakken.**
  Thuis geen versnipperaar? Geen klantgegevens opnemen in aantekeningen.

***Dumpsterdiving:*** *Criminelen vissen de papierbakken op de luchthaven leeg, op zoek naar persoonsinformatie. Zo proberen ze met jouw oude instapkaart je identiteit te vervalsen.*
*Let dus goed op wat je weggooit en waar.*



# Privacy

Privacy gaat over het beschermen van persoonsgegevens. We vertrouwen erop dat de overheid goed met onze naam en ons BSN omgaat. Dit vertrouwen geven we ook aan bedrijven als we akkoord gaan met het plaatsen van cookies bij ons bezoek aan een website. Maar heb je enig idee wat er gebeurt met de informatie die door die cookies over je verkregen is? Wat weet jij van trackers en hoe kun je handelen in data?

***Leestip:*** *In 'Je hebt wél iets te verbergen: over het levensbelang van privacy' laten onderzoeksjournalisten Maurits Martijn en Dimitri Tokmetzis zien dat privacy het meest bedreigde mensenrecht van onze tijd is. Ze leggen bloot welke gegevens je allemaal weggeeft en aan wie. En belangrijker nog: welke ingrijpende gevolgen dat heeft.*

# Herken de risico's in je werk



## Checklist

**Weet ik dit?**

- ☐ *Ik weet wat een datalek is*
- ☐ *Ik weet hoe ik een valse e-mail herken*
- ☐ *Ik controleer of websites veilig zijn*
- ☐ *Ik ken de risico's van openbare WiFi*

# Tip 4: Wat is een datalek?

De wetgeving over privacy is zeer streng. Daarom is het belangrijk om heel zorgvuldig met persoonsgegevens om te gaan. Het verlies van persoons-gegevens noemen we een datalek. Voorbeelden van datalekken zijn:

- **Je verliest een USB-stick met de ledenlijst van je sportclub.**
- **Je raakt een personeelsdossier kwijt (ook papieren informatie valt onder data).**
- **Je stuurt per ongeluk een e-mail met verzuimgegevens van medewerkers naar een verkeerde persoon.**
- **Je computer met alle klantgegevens is gegijzeld en je hebt geen toegang tot een kopie.**

Herken of vermoed je een datalek?
Meld het dan direct via het selfserviceportal van het CAK.




# Tip 5: Herken phishing e-mails

Als je op een phishing e-mail klikt, kan de schade groot zijn. Je bestanden kunnen gegijzeld worden (ransomware), informatie kan ongemerkt worden afgetapt of een virus kan op je PC terecht komen (malware).

- **Je wordt gevraagd om geld over te boeken of een rekeningnummer te wijzigen door een collega of manager.**
  Wees alert als je gevraagd wordt om geld over te boeken of een rekeningnummer te wijzigen door een collega of manager. Dit soort processen verlopen normaal niet via e-mail.
- **Let op de afzender van de e-mail.**
  Kijk niet naar de naam, maar naar het e-mail adres dat er naast staat.
- Klik niet op links en open geen bijlages van onbekende afzenders.
  Bijlages en links kunnen virussen bevatten, open ze niet !
- **Laat je niet onder druk zetten of verleiden.**
  Vaak worden tijdsdruk en winacties ingezet om je op links te laten klikken of in te laten loggen. Let extra goed op !
- **Log niet in via de link in de e-mail.**
  Gebruik de link uit de e-mail niet om in te loggen bij de website.
  Ga zelf naar de URL die je al kent en log vanaf daar in.

**Er zijn meer vormen van phishing:**

- **Telefonische phishing.**
  Word je gebeld en vraagt de beller om je gegevens (te checken)? Wees alert, trap er niet in. Telefonische phishing kan ook worden gebruikt om e-mail phishing betrouwbaarder te laten lijken.
- **Phising via SMS, Whatsapp, Teams, brief…**
  Phishing kan ook worden uitgevoerd via SMS of WhatsApp of via meerdere kanalen tegelijk. Wees hier alert op.
- **Consent phishing.**
  Hierbij worden apps in de Office 365, de Google workspace omgeving of op je telefoon gebruikt om toegang tot je gegevens te verkrijgen.
  Let goed op welke apps je waartoe toegang geeft. Zie voor meer info: https://www.digitaltrustcenter.nl/wat-is-consent-phishing.

# Waar je ook bent, wees alert online!

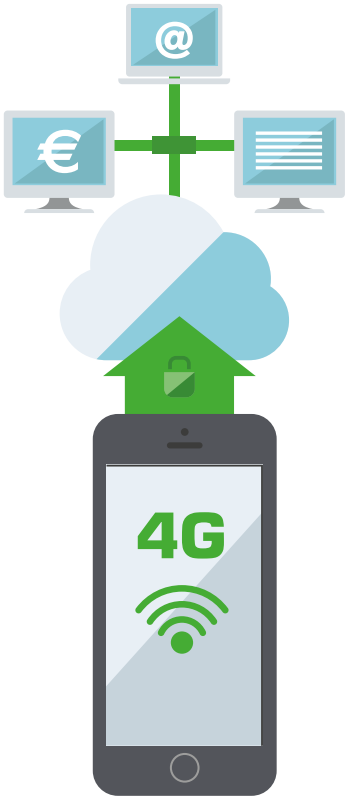
## Tip 6: Check de URL

Controleer of de URL die jij bezoekt inderdaad de URL is die jij wilt bezoeken! Criminelen gebruiken namen die op de officiële naam lijken, bijvoorbeeld: **het-cak.nl** in plaats van **hetcak.nl.**

## Tip 7: Gebruik je mobiele netwerk

- **Gebruik je mobiele netwerk of de hotspot** van je mobiele telefoon (met wachtwoord) in plaats van openbare- of onbekende WiFi.

  Een mobiel netwerk is beveiligd en versleutelt de informatie.





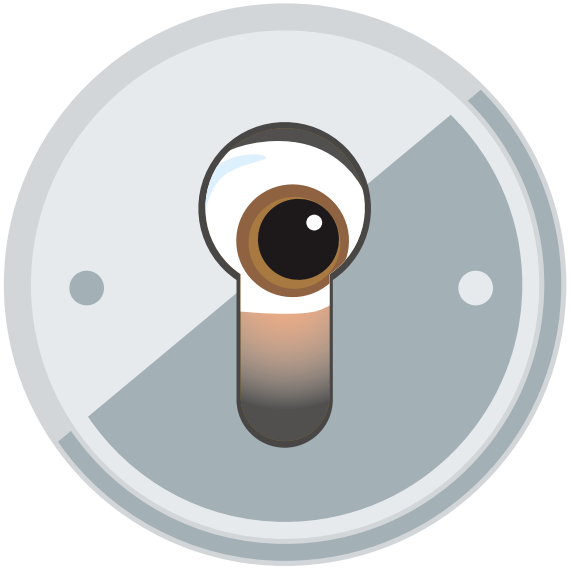

## Tip 8: Met elkaar maak je het veilig

Samen bouw je aan een (informatie)veilige omgeving. Geef elkaar feedback en zorg dat je een veilige basis hebt en houdt. Maak afspraken over het ontvangen van gasten, het gebruik van toegangspassen en bijvoorbeeld het afsluiten van je scherm.

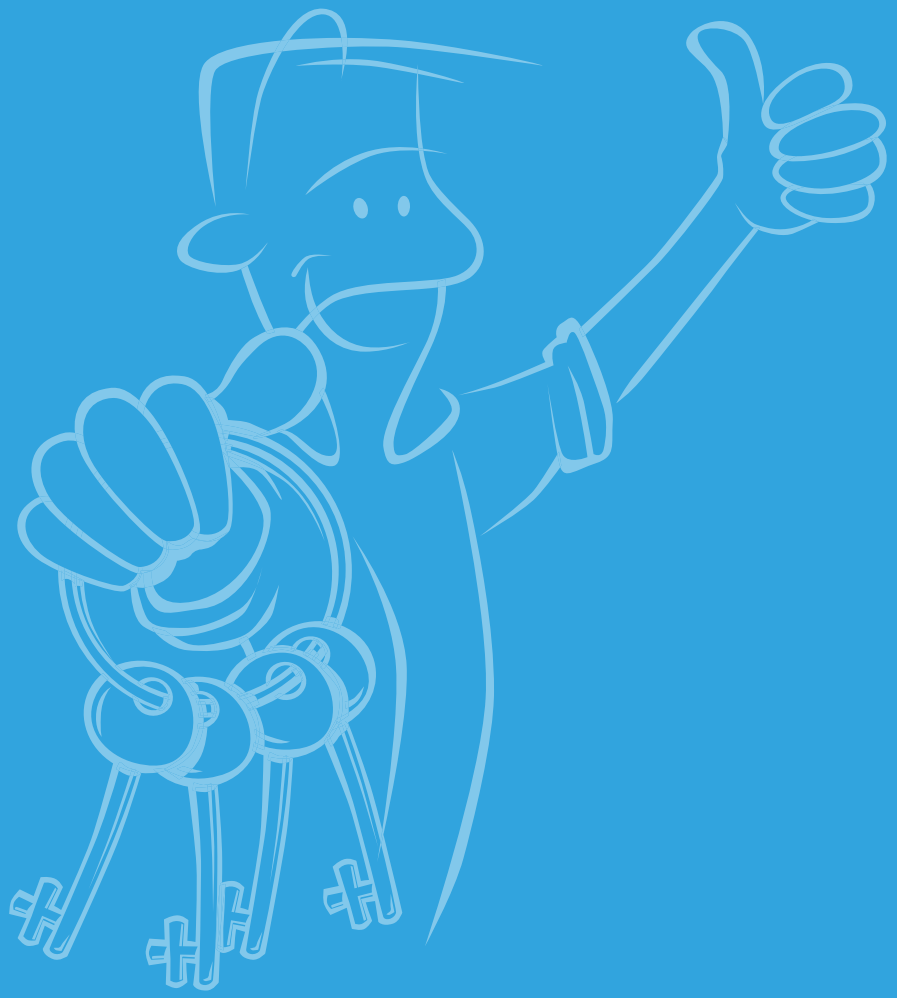
Insluipen gaat vaak heel makkelijk.

**Loopt er iemand over je afdeling die je niet kent?**

- **Vraag aan de persoon met wie hij of zij een afspraak heeft.** Begeleid de persoon naar de desbetreffende collega.
- **Vraag de persoon in kwestie mee te gaan naar de receptie.** De receptionist kan het verder afhandelen.



# Expert tips: extra maatregelen voor meer veiligheid





## Checklist

**Doe ik dit?**

- ☐ *Ik gebruik een wachtwoordmanager*
- ☐ *Ik gebruik 2-factor authenticatie*
- ☐ *Ik houd mijn kennis op peil*
- ☐ *Ik installeer updates*
- ☐ *Ik maak backups*
- ☐ *Ik verwijder wat niet nodig is*
- ☐ *Ik houd ongewenste meekijkers tegen*

# Tip 9: Wachtwoordmanagers

Wachtwoorden kun je veilig beheren met een wachtwoordmanager. Zodat je voor ieder doel of iedere website een ander wachtwoord kunt kiezen en sterkere wachtwoorden kunt gebruiken. Deze wachtwoorden hoef je niet zelf te onthouden, dit doet de wachtwoordmanager voor je. De toegang tot de wachtwoordmanager stel je in met een sterk hoofdwachtwoord, deze moet je natuurlijk wel onthouden.

Gebruik de wachtwoordmanager van het CAK voor al je zakelijke wachtwoorden.



# Tip 10: 2-factor authenticatie

Bij 2-factor authenticatie maak je bij het inloggen naast je wachtwoord (iets dat je weet) nog gebruik  van een andere factor (iets dat je hebt of iets dat je bent). Dit biedt extra bescherming voor je accounts. Bekende vormen van 2-factor authenticatie zijn het gebruik van een authenticatie app (SecureID, Google Authenticator, Microsoft Authenticator, Authy) en SMS.

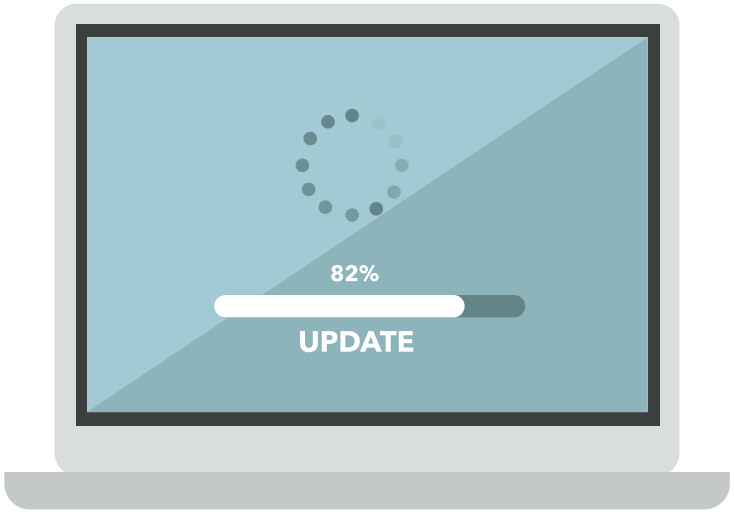
Hierbij heeft de authenticatie app de voorkeur omdat SMS slecht beveiligd is. Stel 2-factor authenticatie in waar mogelijk.

# Tip 11: Spijker je kennis regelmatig bij Direct naar de CAK Academie >

De overheid wil iedereen helpen om veilig op het web te kunnen samenwerken, met vrienden te socializen en aan- en verkopen te doen. Kijk voor nog meer handige tips op https://veiliginternetten.nl/

# Tip 12: Installeer updates

Houd al je software en dus ook je apps up-to-date. De leverancier doet er alles aan om lekken in de software dicht te maken, maar dat helpt alleen als je de laatste updates ook echt installeert. Werk daarom direct je software en je apps bij, als er updates worden aangeboden. Doe dit het liefst automatisch.




# Tip 13: Maak backups

Maak regelmatig backups. Een backup is een reservekopie van je gegevens. Mocht er iets gebeuren, zoals gijzeling van bestanden door ransomware, of diefstal van je apparaat, dan heb je in ieder geval nog een backup. Het is knap frustrerend als je vakantiefoto's en administratie zijn verdwenen.



# Tip 14: Verwijder het overbodige

Heb jij accounts, rechten, documenten, software, toestellen, informatie die je niet nodig hebt? Verwijder ze maar! Met minder accounts en documenten verklein je het risico op hacking en datalekken.

Dit is ook een privacy principe: persoonsgegevens moeten worden verwijderd op het moment dat ze niet meer nodig zijn

# Tip 15: Camera blokkeren

Je camera wordt door software (zoals Skype) gebruikt voor het maken van filmpjes of foto's. Er bestaan apps die dit ongemerkt doen. Bijvoorbeeld om je te chanteren met de beelden. Wil je zelf controle hebben over je camera? Gebruik dan een handig schuifje (webcamcover) om je camera af te dekken.

**Specifiek voor het werken op een andere locatie dan bij het CAK gelden extra risico's, dus daarom extra tips:**

**Tip 16:** Voorkom meekijken op je scherm door derden.

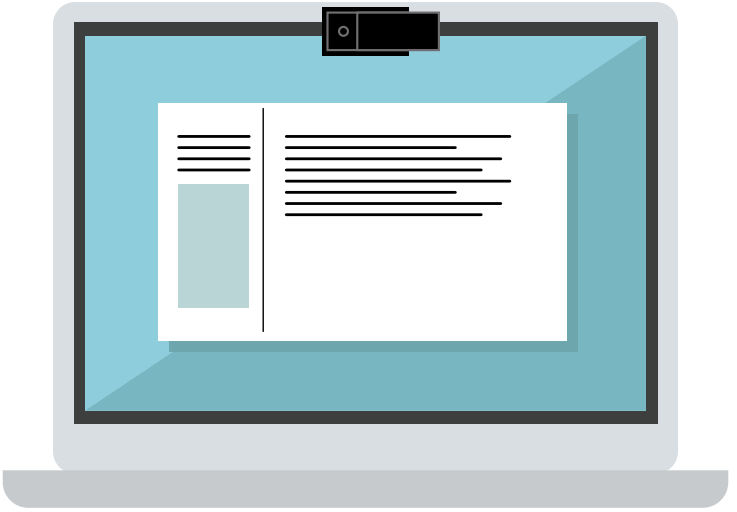
**Tip 17:** Maak geen gebruik van onbeveiligde netwerken (station, McDonald's).

**Tip 18:** Vertrouwelijke gesprekken aan de telefoon? Let op wie er mee kan luisteren.



**Tip 19:** Klantgegevens nooit gebruiken in MS Teams, CAK testomgevingen, WhatsApp, Signal, Trello, Dropbox, etc., maar alleen in de door het CAK beveiligde omgeving.

**Tip 20:** Noteer zo min mogelijk klantgegevens. Vernietig aantekeningen aan het eind van de werkdag.



# EHBO: Nuttige adressen

## Ondanks alle goede zorgen, kan er nog steeds iets misgaan. Het is daarom belangrijk dat je weet waar je terecht kunt met vragen.

| **Ik vermoed** | **Ik neem meteen contact op met:** |
|---|---|
| *Gijzelsoftware* | In alle hiernaast genoemde gevallen melden via het SelfServicePortal van het CAK. |
| *Een phishing e-mail* | |
| *Een gevonden USB stick* | |
| *Een datalek* | |

LBVD

Versie: september 2023