



Oost west, thuis best

Werk ook thuis veilig

Brussel, september 2020

Hallo en welkom allemaal!

Thuiswerken
kan een uitdaging zijn.



Herkent u dit ?

BBC Interview met medewerking van de
kids thuis...





**ER WAS EENS
EEN VREDIG
KONINKRIJK**

WAAR HET
VOOR ALLE
THUISWERKERS
HEERLIJK
TOEVEN WAS





Telewerken

mag niet betekenen dat jij en je organisatie een groter gevaar lopen om slachtoffer te worden van een cyberaanval



Check de module 'Wachtwoorden' in de Cyber Security Kit

 **CYBER SECURITY COALITION**_{be}

Voorwaarden om veilig te kunnen thuiswerken...

Goed beveiligde en krachtige netwerkverbinding (1/2) :

- Installeer een VPN (Virtual Private Network)
- Verander de standaardwachtwoorden van al je apparaten, ook de domotica. Hoe maak je sterke wachtwoorden: zie module 'Wachtwoorden' in deze Cyber Security Kit.
- Beveilig je router goed
- Activeer de firewall en bescherm je computer en smartphone met een virusscanner
- Schakel WPS (Wi-Fi Protected Setup) uit

(Bronnen: www.safeonweb.be, Vrije Universiteit Brussel, BNP Paribas Fortis, US Department of Homeland Security)

We gebruiken iedere dag internet via onze smartphone, tablet, pc maar ook steeds meer met 'slimme' apparaten zoals camera's, tv en domotica-oplossingen. Maar deze afhankelijkheid brengt risico's met zich mee. Hoe bescherm ik mijn thuisnetwerk tegen ongewenste gebruikers?

Een goed beveiligd netwerk betekent:

- Installeer een **Virtual Private Network (VPN)**. Dit is je persoonlijke **beveiligde tunnel door het wifinetwerk**. Alle communicatie verloopt door een versleutelde virtuele tunnel, die vermijdt dat cybercriminelen leesbare communicatie kunnen onderscheppen en zo de informatie kunnen bemachtigen. Vele werkgevers voorzien een betrouwbare VPN verbinding voor hun werknemers zodat die veilig toegang kunnen krijgen tot het professionele netwerk. Is dat niet het geval, dan kan je zelf online gratis of betalend VPN diensten installeren. Verschillende virusscanners bieden bv. VPN aan.
- Verander de standaardwachtwoorden van **al** je apparaten die op je thuisnetwerk zijn aangesloten. Dat kunnen onder meer computers, smartphones, tablets, printers zijn, maar ook bijvoorbeeld camera's en netwerksystemen die al deze apparaten eenvoudig met elkaar via jouw thuisnetwerk verbinden. 'Admin' en 'password' zijn voorbeelden van zwakke standaardwachtwoorden, die helaas nog vaak worden gebruikt. Hoe maak je sterke wachtwoorden: zie module 'Wachtwoorden' in deze Cyber Security Kit.
- Beveilig je router goed: **De router is de poort tussen het internet en je thuisnetwerk: beveilig hem goed.**
- Wijzig de netwerknaam van je home WiFi(SSID)** en verwerk er geen evidente elementen in zoals je adres. Een cybercrimineel kan dan vanop de openbare weg zien welk netwerk bij welk huis hoort. Soms is de producent

van je apparaten ook verwerkt in de netwerknaam, ook zo zet je voor hackers de deur open.

- Wijzig je netwerkwachtwoorden** (inclusief het wachtwoord dat op je router staat).
- Gebruik WPA2 beveiliging.** Je router heeft waarschijnlijk de mogelijkheid om WPA3, WPA2, WPA of WEP **versleuteling** in te stellen. Kies het veilige WPA2 of WPA3 (**WiFi Protected Access**) en stel dit onmiddellijk in met een sterk en lang wachtwoord als dit nog niet gebeurd is. Zo ben je er zeker van dat **alleen mensen die je vertrouwt verbinding kunnen maken** met je thuisnetwerk. Want je bent dan verplicht om een wachtwoord in te voeren. Bovendien zijn alle online activiteiten dan versleuteld.
- Update alle apparatuur.** Je router is ook een computer en krijg ook updates net zoals je computer. Zorg dat de laatste updates geïnstalleerd zijn op je router en andere netwerkkaparaatuur.

(*) **Hoe kan je de instellingen van je router wijzigen?**

[Proximus](#)

[Telenet](#)

- Activeer de firewall en gebruik altijd een [virusscanner](#).**
- Schakel WPS (Wi-Fi Protected Setup) uit.** WPS is een functie die toestellen op een eenvoudigere manier laat verbinden met een wifinetwerk zonder daarvoor een wachtwoord in te voeren. Criminelen kunnen dit misbruiken om een verbinding te maken met je netwerk. Als je voor langere periode niet thuis bent, zet dan je WiFi-netwerk af.

Telewerken

mag niet betekenen dat jij en je organisatie een groter gevaar lopen om slachtoffer te worden van een cyberaanval



Check de module 'Wachtwoorden' in de Cyber Security Kit



Voorwaarden om veilig te kunnen thuiswerken...

Goed beveiligde en krachtige netwerkverbinding (2/2) :

- Maak een gastnetwerk
- Gebruik indien mogelijk de 'vaste internetlijn' of Ethernet
- Vermijd buitenshuis publieke WiFi in hotels, luchthavens, stations, cafés
- Installeer indien nodig een WiFi booster
- Koop alleen apps in officiële app-stores
- Zorg dat je besturingssysteem, al je programma's & apps up-to-date zijn en zorg ervoor dat de updates automatisch geïnstalleerd worden

(Bronnen: www.safeonweb.be, Vrije Universiteit Brussel, BNP Paribas Fortis, US Department of Homeland Security)

- Maak een gastnetwerk.** Een gastnetwerk is een apart wifinetwerk dat strikt gescheiden is van het eigen netwerk. Je gasten krijgen daarmee wel toegang tot je internetverbinding, maar niet tot je gedeelde bestanden en apparaten zoals printers en netwerk harde schijven. Je kunt het wachtwoord voor je gastnetwerk dus ook met een gerust hart delen. Veel routers bieden deze mogelijkheid via de instellingen. Maak je netwerk nog veiliger door je 'slimme' iot-apparaten (Internet of Things - apparaten verbonden met het internet en zo op afstand aan te sturen zoals lampen, thermostaat...) alleen met het gastnetwerk te laten verbinden. Daardoor hebben hackers, die misbruik maken van een iot-lek, minder eenvoudig toegang tot je hele netwerk.
- Gebruik de 'vaste internetlijn' of Ethernet.** Gebruik een ethernetkabel in plaats van wifi voor toestellen die je niet verplaatst, zoals desktopcomputers, tv's of printers. Een draadloos netwerk, zelfs wanneer het beveiligd is, kan gekraakt worden door iemand die zich binnen het bereik bevindt. Wifi zendt en ontvangt nu eenmaal radiosignalen binnen een ruim bereik, en dat is een potentieel veiligheidsrisico. Gegevens die door een kabel gaan kunnen hackers veel moeilijker onderscheppen omdat daar fysieke toegang voor nodig is.
- Vermijd buitenshuis publieke WiFi** in hotels, luchthavens, stations, cafés
- Installeer indien nodig een WiFi **booster om een sterke internetconnectie te garanderen** in je home office.
- Koop alleen apps in **officiële app-stores** (App Store, Google Play).
- Zorg dat je **besturingssysteem, al je programma's en apps up-to-date** zijn. Software die niet meer ondersteund wordt door de leverancier krijgt ook geen beveiligingsupdates meer. Oude besturingssystemen zoals bijvoorbeeld Windows XP of Windows 7, oude emailprogramma's, of elke andere software die niet langer ondersteund wordt vormt een zeer belangrijk beveiligingsrisico. Zorg dat je anti-virus **de updates automatisch installeert**.

Thuiswerken op je huislaptop?

Organisaties die al langer telewerk voorzien, bezorgen hun werknemers laptops en eventueel ook smartphones van het bedrijf.



Voorwaarden om veilig te kunnen thuiswerken...

Een veilige werkomgeving (1/2) :

- Gebruik bij voorkeur de laptop/smartphone van je werkgever als deze beschikbaar zijn.
- Als je je privé apparaten kan gebruiken, sluit dan alle privé vensters en applicaties tijdens je werksessies.
- Installeer veilige communicatietools als je veel vertrouwelijke informatie deelt met collega's.
- Niet alle Apps zijn veilig: volg de richtlijnen van je IT-afdeling of vraag het advies van je IT-leverancier

(Bronnen: www.safeonweb.be, Vrije Universiteit Brussel, US Department of Homeland Security & BNP Paribas Fortis)

- Gebruik bij voorkeur de laptop/smartphone van je werkgever. Die zijn **beter beveiligd en gecontroleerd** dan je eigen apparaten. Bovendien kan je werkgever **onmiddellijk ingrijpen** wanneer zich een probleem voordoet. Op de apparaten van je werkgever is doorgaans antivirussoftware actief en gebeuren de updates automatisch. Je bent je als werknemer hiervan niet altijd bewust. Voor je privé-toestellen ben je hier zelf verantwoordelijk en dat wordt somst vergeten.
- Als je je privé apparaten kan gebruiken, volg dan de instructies van je werkgever, **sluit ook alle privé vensters en applicaties tijdens je werksessies**.
- **Installeer veilige communicatietools (volg de richtlijnen van je IT-departement of vraag het advies van je IT-leverancier) als je veel vertrouwelijke informatie deelt met collega's.** Om berichten te versturen, maken collega's vaak gebruik van WhatsApp. Threema of Telegram bv. zijn minder bekende maar beter beveiligde alternatieven. Voor videogesprekken bestaan er alternatieven voor bv. Skype (Zoom, Teams, Webex,...). Lees het NVISO-advies over Zoom: : [to Zoom or not to Zoom](#)
- **Niet alle Apps zijn veilig: volg de richtlijnen van je IT-afdeling of vraag het advies van je IT-leverancier).** Als je IT-afdeling bv. verbiedt om confidentiële info te delen via WhatsApp of om grote bestanden via WeTransfer te versturen, volg dan deze richtlijnen: ze zijn weldoordacht en hebben als bedoeling het risico op bv. informatielekken te beperken. In de meeste gevallen zijn er ook valabele alternatieven beschikbaar.

Thuiswerken op je huislaptop?

Organisaties die al langer telewerk voorzien, bezorgen hun werknemers laptops en eventueel ook smartphones van het bedrijf, dat is veiliger dan met privé-apparaten te werken.



CYBER SECURITY COALITION_{be}

Voorwaarden om veilig te kunnen thuiswerken...

Een veilige werkomgeving (2/2): Bewaak je privacy en discretie in je home office

- Druk thuis geen werk-gerelateerd materiaal af tenzij dit expliciet wordt toegestaan door je IT-afdeling.
- Vergrendel je computer als je de werkplek verlaat, beveilig je smartphone met een pincode.
- Sluit je computer elke avond af
- Laat geen wachtwoorden rondslingeren
- Voer vertrouwelijke gesprekken buiten het bereik van luistervinken
- Laat je kinderen of bezoekers niet op je werkpc of -smartphone toe

(Bronnen: www.safeonweb.be, Vrije Universiteit Brussel & BNP Paribas Fortis)

Een veilige werkomgeving betekent dat je je privacy en discretie in je home office goed bewaakt. Concreet kan dit a.v.:

- **Druk thuis geen werk-gerelateerd materiaal af** tenzij dit expliciet wordt toegestaan door je IT-afdeling.
- **Vergrendel je computer als je de werkplek verlaat:** Thuis maar ook op kantoor is het een goede gewoonte om je computer steeds te vergrendelen als je je werkplek verlaat, zodat niemand de kans krijgt om in je bestanden te snuffelen. Ook met spelende kinderen in de buurt, nieuwsgierige pubers of een kat die gek is op je toetsenbord, is het verstandig om steeds je toestel te vergrendelen als je even weg bent. Vergrendelen doe je eenvoudig met de toetsen WIN+L of Ctrl + Shift + Power voor Mac-gebruikers. Activeer ook een pinbeveiliging op je smartphone.
- **Sluit je computer elke avond af.** Weersta aan de verleiding om 's avonds je computer in slaapstand te zetten zodat je 's ochtends weer snel aan de slag kan. Als je je computer afsluit, worden nieuwe updates uitgevoerd. Een deel van die updates betekenen een verbetering in de beveiliging. Het is dus belangrijk dat je deze updates regelmatig uitvoert.
- **Laat geen wachtwoorden rondslingeren:** Het spreekt voor zich dat je geen post-it met je wachtwoorden aan je scherm kleeft. Maar ook een discreet papiertje onder je toetsenbord is geen goed idee. Het is natuurlijk een onmogelijke zaak om de wachtwoorden van je persoonlijke en professionele accounts te onthouden. Bewaar je wachtwoorden daarom in een online wachtwoordkuis (een wachtwoordmanager) die je beveiligd met een sterke wachtwoordzin. Je moet voortaan maar 1 wachtwoord onthouden. Maak waar mogelijk gebruik van Two-Factor Authentication (2FA) <https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden>
- **Voer vertrouwelijke gesprekken buiten het bereik van luistervinken.** Als je thuis of op de trein telefonische gesprekken voert, zorg er dan voor dat derden niet kunnen meeluisteren. Het is niet de bedoeling dat op die manier informatie over je werk, je klanten of je bedrijf publiek wordt. Zorg dat je thuis ook een plek hebt waar je discreet kan telefoneren.
- **Laat je kinderen of bezoekers niet op je werkpc of -smartphone toe.** De verleiding is soms groot om je kinderen te laten werken/spelen/les volgen op je werkpc, maar hiermee verhoog je de veiligheidsrisico's. Op kantoor hoef je je immers geen zorgen te maken over kinderen, gasten of andere gezinsleden die je werk-laptop of de systemen van je werkgever gebruiken. Draag er zorg voor dat bij thuiswerken het duidelijk maakt voor familie en vrienden dat ze je werksystemen niet kunnen gebruiken. Informatie zou per ongeluk gewist of gewijzigd kunnen worden, of het systeem kan in het ergste geval per ongeluk geïnfecteerd geraken.

Fake news en phishing berichten

Cybercriminelen spelen in op de actualiteit en weten welke thema's ons interesseren



Check de module 'Phishing' in de Cyber Security Kit



Voorwaarden om veilig te kunnen thuiswerken...

Herken valse berichten op tijd:

- Klik niet op de links of afbeeldingen in valse berichten en open geen bijlagen. Als je twijfelt, zoek de website op via een zoekmachine. Bekijk de module 'Phishing' van deze Cyber Security Kit.
- Download geen onofficiële software op je computer of apps op je smartphone buiten de officiële App Store/Google Play
- Contacteer onmiddellijk je IT-afdeling of je IT-leverancier als je toch op een link of een bijlage in een verdacht bericht geklikt hebt
- Draag niet bij aan de verspreiding van valse berichten die je vrienden en familie alleen maar bang kunnen maken.
- Stuur verdachte berichten door naar verdacht@safeonweb.be of naar de phishing-mailbox van je bank.

(Bronnen: www.safeonweb.be & BNP Paribas Fortis)

Herken valse berichten op tijd

Besteed speciale aandacht aan de e-mails die je ontvangt. De remedie tegen het coronavirus bv. wordt niet via e-mail geleverd. Het Centrum voor Cybersecurity België (CCB) krijgen momenteel verschillende meldingen van valse berichten over het coronavirus:

- met aanbiedingen over mondkapjes
- met valse geldinzamelacties voor slachtoffers van het virus
- met links naar valse nieuwssites
- met aanbiedingen over vaccins

Ga op zoek naar correcte informatie. De officiële berichten van de FOD Volksgezondheid vind je op de website info-coronavirus.be.

Wat doen als je een vals bericht krijgt ?

- Klik niet op de links of afbeeldingen in valse berichten en open geen bijlagen. **Bijlagen downloaden of links openen** in e-mails doe je alleen wanneer ze afkomstig zijn van **gekende en betrouwbare bronnen**. Doe dat niet als ze van andere bronnen komen, ook al lijkt het bericht nog zo dringend of uitnodigend.
- Als je twijfelt, zoek de website op via een zoekmachine.
- Open zeker geen documenten en bijlagen van onbevestigde officiële bronnen over de COVID-19, op welk apparaat dan ook.
- Download geen onofficiële software op je computer of apps op je smartphone buiten de officiële App Store om meer te weten te komen over COVID-19.
- Draag niet bij aan de verspreiding van valse berichten die je vrienden en familie alleen maar bang kunnen maken.
- Stuur verdachte berichten door naar verdacht@safeonweb.be** of naar de phishing-mailbox van je bank.

Wat doen als je toch op een link of bijlage in een verdacht bericht geklikt hebt ?

Vermoed je dat iemand je wachtwoord kent, of dat je op je e-mailadres of telefoon van je werkgever phishingmail hebt ontvangen? Heb je toch op een link of een bijlage in een verdacht bericht geklikt? Is je laptop, smartphone of tablet van je werkgever verloren geraakt of gestolen? Meld dat dan onmiddellijk aan je werkgever.

Werk en privé?

Ook als thuiswerker moet je duidelijk het onderscheid blijven maken tussen privé en professionele communicatie



Check de module 'Social Engineering' in de Cyber Security Kit

 CYBER SECURITY COALITION_{be}

Voorwaarden om veilig te kunnen thuiswerken...

Veilig communicatiekanalen gebruiken:

- Gebruik voor werkcommunicatie alleen de applicaties die door je IT-afdeling of je IT-leverancier geselecteerd zijn.
- Stuur geen werkmails naar je privé G-mail/ Hotmail account: risico op informatielek
- Gebruik steeds een HTTPS-verbinding
- Zet geen werkinfo op social media
- Berg vertrouwelijke documenten veilig op in afwachting dat je ze terugbrengt naar je werk.

10

(Bron: Vrije Universiteit Brussel & BNP Paribas Fortis)

Veilig communicatiekanalen gebruiken

- Gebruik voor werkcommunicatie **de applicaties die door je IT-afdeling of IT-leverancier geselecteerd zijn.**

Communicatiemiddelen zijn belangrijk bij het thuiswerken. De VPN van je werkgever (zie slide 4) laat je toe om je van thuis uit op het netwerk van je werkgever aan te sluiten. Maar er zijn ook nog heel veel andere communicatiemiddelen. Wat van heel groot belang is, is dat je een heel duidelijk onderscheid maakt tussen privé- en werkcommunicatie en dat je deze vooral niet mengt. Voor je werkcommunicatie gebruik je best enkel applicaties die door de werkgever geselecteerd werden. Gebruik erkende producten uit een officiële appstore en zorg dat ze up-to-date zijn.

- Stuur geen werkmails naar je privé G-mail/ Hotmail account: **risico op informatielek**

Verstuur je e-mail voor je werk, dan gebruik je enkel je werkaccount. Soms lijkt het handig om snel een bestandje naar je eigen Gmail/Hotmail-account te sturen zodat je het document thuis kan afprinten. Denk eraan dat hierdoor werk gerelateerde gevoelige informatie gelekt kan worden. Je homeprinter voldoet immers niet altijd aan de veiligheidsvereisten van je werkgever. Doe dit dus in geen geval! Wees extra op je hoede wanneer je extern communiceert en informatie uitwisselt. Maak alleen gebruik van oplossingen die zijn goedgekeurd.

- Gebruik steeds een **HTTPS-verbinding**

Surf je naar websites, let er dan op dat je browser **steeds een HTTPS en geen HTTP-verbinding** gebruikt. Doe dit zeker als je persoonlijke gegevens op die website moet ingeven, zoals je gebruikersnaam en wachtwoord. HTTPS gebruikt een versleutelde en beveiligde communicatie. Dit is niet het geval voor een HTTP-verbinding, waarbij al jouw ingevoerde gegevens integraal en zonder versleuteling over het internet verstuurd worden en die bijgevolg door cybercriminelen onderschept kunnen worden.

- Zet **geen werkinfo op social media**

Bij thuiswerken is de grens tussen gebruik van je (privé) sociale media en werkactiviteiten minder vanzelfsprekend dan op het kantoor. Het online zetten van kleine werkdetails of je dagelijkse routine lijkt minder raar als er geen collega's zijn waarmee je die dingen kan delen. Thuiswerkers moeten hiermee toch oppassen, want zo'n updates bieden vaak waardevolle informatie voor het opzetten van phishing-campagnes.

- Berg **vertrouwelijke documenten** veilig op in afwachting dat je ze terugbrengt naar je werk. Gooi ze niet bij je huishoudelijk papierafval. Op je werk kunnen deze documenten in vele gevallen discreet worden vernietigd/verwerkt.

Alles online?

Lesgeven, vergaderen en zelfs aperitieven met vrienden gebeurt nu zonder verpinken online.




Voorwaarden om veilig te kunnen thuiswerken...

Veilig online videoconferenties houden (1/2):

- Gebruik erkende producten uit een officiële appstore en zorg dat ze up-to-date zijn
- Maak een eigen account aan en beveilig die met een sterk wachtwoord
- Hou je telefoon- en videogesprekken vertrouwelijk
 - Waar je ongestoord kan praten
 - Let op je 'visuele' en 'audio' omgeving thuis: geen gevoelige info prijs.
 - Enkel met genodigde gasten
 - Bescherm elke vergadering met een wachtwoord
 - 'Lock' het event zodra alle genodigden aanwezig zijn
 - Gebruik je koptelefoon
 - Gebruik webcamcover

(Bronnen: www.safeonweb.be & US Department of Homeland Security)

Veilig online videoconferenties houden:

- Gebruik erkende producten uit een officiële appstore en zorg dat ze up-to-date zijn.
 - Als je een app uit een appstore downloadt, gebruik dan enkel de **officiële appstores** (App Store/Google Play)
 - Welk platform je ook gebruikt, zorg dat je **updates** steeds uitvoert. Bij een update worden meer functionaliteiten voorzien en fouten opgelost. Ook de kwetsbaarheden in de beveiliging worden bij een update verholpen. Daarom is het belangrijk om updates steeds uit te voeren als daar naar gevraagd wordt.
- Maak een **eigen account** aan en beveilig die met een **sterk wachtwoord**.
- Hou je telefoon- en videogesprekken **vertrouwelijk**.
 - Voer videogesprekken **op een plaats waar je ongestoord kan praten**. Als je op je terras vergadert, kunnen de burens misschien elk woord opvangen en dat is niet de bedoeling. Hetzelfde geldt voor de trein of een andere openbare plaats.
 - Let op je **'visuele' en 'audio' omgeving** thuis: geen gevoelige info prijs. Maak gebruik van de mogelijkheid om de achtergrond te vervagen of te vervagen ('blurring').
 - **Deel de link naar de meeting enkel met genodigde gasten** en niet in het openbaar (bv. op Facebook). Zo voorkom je dat er ongewenste deelnemers komen opdagen. Zorg ervoor dat je als 'host' alle aanwezigen kan 'muten' (micro uitschakelen), dat doe je best in het begin, en kan bepalen wie er schermen deelt.
- **Bescherm elke vergadering met een wachtwoord**. Gebruik de 'wachtkamer' om de toegang van je gasten te controleren. Wees als gastheer/vrouw de eerste, laat andere deelnemers niet binnen vóór jou.
- 'Lock' het event zodra alle genodigden aanwezig zijn, zo vermijd je niet-gewenste pottenkijkers.
- Gebruik je **koptelefoon** en zet eventuele veiligheidscamera's in je woning af.
- **Gebruik een webcamcover**. Zorg ervoor dat je webcam altijd afgedekt is als je hem niet gebruikt.
- **Bescherm je gegevens** optimaal.
 - Voor het delen van zeer gevoelige informatie heb je misschien een hogere bescherming nodig. Bekijk hiervoor de **specificaties en instellingen**.
 - Vraag aan je werkgever om **veilige communicatiekanalen** te installeren als je veel vertrouwelijke informatie deelt met collega's.
- Als je **bestanden, schermen deelt of wanneer je de meeting opneemt**: let ook dan op dat je dit zeer gecontroleerd doet. Weet wie er meekijkt/-luistert. Let ook op als je je volledige scherm deelt of een individuele toepassing.
- Denk goed na over de gevoeligheid van de info voor je ze deelt via je scherm. **Besprek geen info die je ook niet via de telefoon zou delen**.

Alles online?

Lesgeven, vergaderen en zelfs aperitieven met vrienden gebeurt nu zonder verpinken online.




Voorwaarden om veilig te kunnen thuiswerken...

Veilig online videoconferenties houden (2/2):

- Bescherm je gegevens optimaal
 - Installeer veilige communicatiekanalen
 - Schermbestanden delen: let op met wie.
 - Deel geen gegevens die je ook niet via telefoon zou delen.

12

(Bronnen: www.safeonweb.be & US Department of Homeland Security)

Veilig online videoconferenties houden:

- Bescherm je gegevens optimaal.**
 - Voor het delen van zeer gevoelige informatie heb je misschien een hogere bescherming nodig. Bekijk hiervoor de **specificaties en instellingen**.
 - Vraag aan je werkgever om **veilige communicatiekanalen** te installeren als je veel vertrouwelijke informatie deelt met collega's.
- Als je **bestanden, schermen deelt of wanneer je de meeting opneemt**: let ook dan op dat je dit zeer gecontroleerd doet. Weet wie er meekijkt/-luistert. Let ook op als je je volledige scherm deelt of een individuele toepassing.
- Denk goed na over de gevoeligheid van de info voor je ze deelt via je scherm. **Bespreek geen info die je ook niet via de telefoon zou delen.**

Thuiswerken

Wat als het misloopt?




Voorwaarden om veilig te kunnen thuiswerken...

Blijf alert en signaleer onmiddellijk onregelmatigheden aan je IT-afdeling, je IT-leverancier, je bank:

- Smartphone, laptop, tablet verloren/gestolen?
- Vermoeden dat je toestel gehackt is?
- Toch geklikt op een link of een bijlage in een verdachte mail?
- Belangrijke info verloren/gestolen?
- Je wachtwoord gehackt?

13

Blijf alert en signaleer onmiddellijk onregelmatigheden aan je werkgever:

- Smartphone, laptop, tablet verloren/gestolen?
- Verdacht bericht?
- Toch geklikt op een link of een bijlage in een verdachte mail?
- Belangrijke info verloren/gestolen?
- Je wachtwoord gehackt?

Signaleer verdachte berichten ook aan verdacht@safeonweb.be. Het CCB zal links naar malafide sites laten blokkeren zodat jij én ook andere gebruikers niet meer in de val kunnen trappen... Als het verdacht bericht vanuit je bank lijkt te komen, stuur het dan naar de phishing mailbox van je bank.

Test hoe veilig je thuiswerkt!

Test je digitale gezondheid

test op www.safeonweb.be



Veilig thuiswerken: skype erover!

Wat is jouw mening?
Heb je opmerkingen?
Wat heb je onthouden?
Je eerste actie?



15

Wat is jouw mening?

Heb je opmerkingen?

Wat heb je onthouden?

Wat zal de eerste actie zijn die je onderneemt na deze presentatie?

Thuiswerken


Aandachtspunten



SANS aandachtspunten


Sans, een belangrijke internationale referentie inzake cyberveiligheid postte [deze video](#) die de belangrijkste boodschappen op deze slides slides bloedserieus maar mooi samenvat:





Nuttige links

- www.safeonweb.be : Centrum voor Cybersecurity België (CCB) met praktische veiligheidstips en tests.
- verdacht@safeonweb.be : verdachte berichten (mail/sms/...) stuur je naar dit adres.
- [Test je digitale gezondheid nu!](#)
- [Webinars over cyberveiligheid](#)
- [Europol: infographies on Covid-19 threats](#) (ENG)
- [Febelfin](#)
- US Department of Homeland Security
- NVISO: [to Zoom or not to Zoom](#)
- SANS: [work from home deployment kit](#)

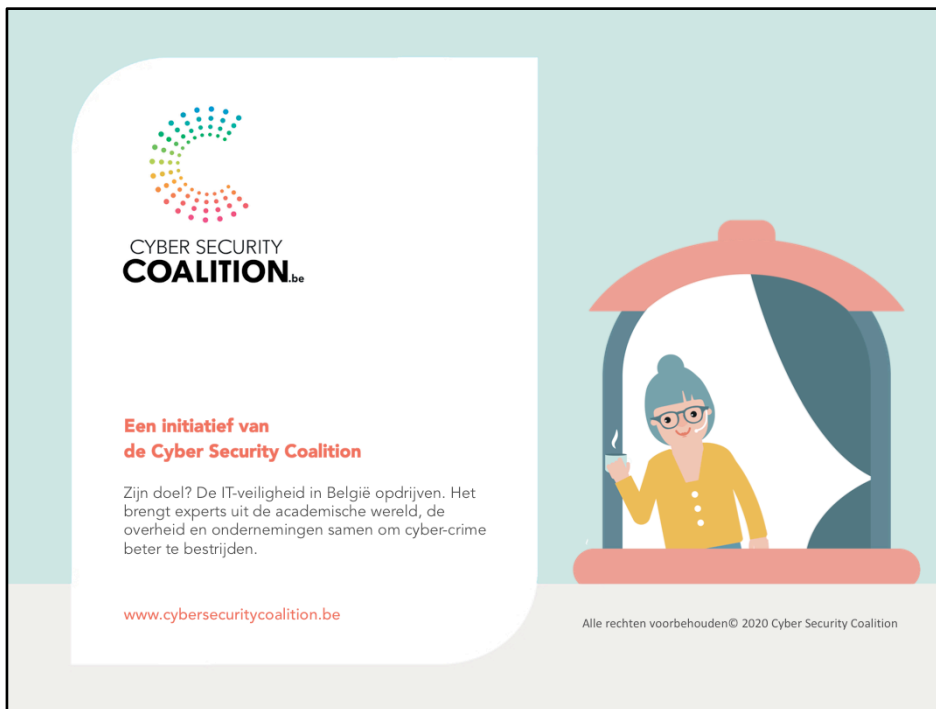
 CYBER SECURITY COALITION.be

17

Nuttige links:

Centrum voor Cybersecurity Belgium (CCB):

- www.safeonweb.be : de website van het Centrum voor Cybersecurity België (CCB) met praktische veiligheidstips en tests.
- verdacht@safeonweb.be : verdachte berichten (mail/sms/...) stuur je naar dit adres. Het CCB laat verdachte linken dan offline halen.
- [Test je digitale gezondheid nu!](#) : Doe de test en ontdek of je digitale gezondheid toe is aan een boost. Je krijgt 15 vragen over updates, back-ups, phishing, virusscans en wachtwoorden.
- [Webinars over cyberveiligheid](#): Deze webinars kunnen organisaties bewust maken van de belangrijkste cyberdreigingen en geven hen praktisch advies om zich te beschermen en klantgegevens te beveiligen. Deze webinars zijn bedoeld voor het management maar ook om alle betrokken werknemers van een organisatie te informeren.
- Europol : <https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know> bevat 4 praktische infografieën (ENG) m.b.t. Covid-19:
 - You can go outside again, criminals can too
 - At home, still spending plenty of time online?
 - Children's safety, a priority
 - Protect your finances
- Febelfin
- US Department of Homeland Security
- NVISO: : [to Zoom or not to Zoom](#)
- SANS: [work from home deployment kit](#)



Bedankt voor je aandacht!