Beste collega,

Voor <**bedrijf**> heeft de gezondheid en veiligheid van jou en onze klanten de hoogste prioriteit. Op dit moment volgen ontwikkelingen met betrekking tot het coronavirus elkaar snel op. We werken allemaal thuis en dat vraagt om een aantal IT-aandachtspunten die we graag met jullie delen. Het gaat hier om alertheid omtrent het gebruik van applicaties en programma’s en de verhoogde activiteit van criminelen die misbruik maken van de thuiswerkers.

**Foto’s of video’s van thuiswerken op social media plaatsen?**

Bij voorkeur: doe het niet. Als je toch dingen deelt, zorg er dan voor dat geen openstaande schermen zichtbaar zijn.

**Videovergaderingen**

Gebruik bij voorkeur de middelen die we jullie hebben aangedragen, **<<Skype, Facetime, GoToMeeting>>.** Belangrijk is dat je als organisator precies weet wie er deelneemt (ook degenen die inbellen). Zodat niemand ongemerkt kan meeluisteren.

**Zorg dat al je apparaten geüpdatet zijn (telefoon, computer en internetrouter)**

Heb je hier vragen over of hulp bij nodig? Stuur dan een e-mail naar: **<<e-mail adres van helpdesk/systeembeheerder/IT verantwoordelijke>>**

**Zorg dat je virusscanner actief en up-to-date is**

Activeer je virusscanner op al je privé-apparatuur en/of werk hem bij.

**Deel vertrouwelijke bestanden op een vertrouwelijke manier**

In deze bijzondere situatie nog belangrijker: **<<gebruik Office365>> <<of Zivver >>**voor het delen van vertrouwelijke bestanden, ook onderling.

**Let op verdachte e-mails of telefoontjes, klik niet op verdachte links**

Ook het coronavirus zelf is een dankbaar onderwerp voor criminelen. We zien bijvoorbeeld dat aan mensen wordt gevraagd gebruik te maken van Microsoft Onedrive. Medewerkers worden naar een nepsite gelinkt, waar ze hun bedrijfsgegevens invullen. Deze worden rechtstreeks naar de crimineel verstuurd. Eenmaal in het systeem, kan een kwaadwillende bestanden versleutelen voor losgeld (ransomware) of zich voordoen als directeur om snel een factuur te laten betalen.

Ook worden e-mails uit naam van het RIVM gestuurd met updates over het virus, of berichten aan ondernemers dat ze in aanmerking komen voor belastinguitstel of compensatie. Nadat deze hun bankgegevens hebben ingevuld, plunderen hackers hun bankrekening in deze toch al zware financiële tijd.

Dus: wees hierop heel alert en meld alle verdachte zaken (ook bij twijfel) via: **<<e-mail adres van helpdesk/systeembeheerder/IT verantwoordelijke>>**

Wij helpen je bij wat je kunt of moet doen.

**Neem voldoende pauze**

Nu je keukentafel je bureau is geworden, is het aantrekkelijk om achter je computer te blijven eten. Toch raden we je aan even achter je laptop vandaan te komen en voldoende pauze te houden. De meeste fouten worden nog steeds door mensen gemaakt. Door af en toe rust te nemen, ben je ook alerter op dit soort dingen.

De huidige situatie vergt flexibiliteit, verantwoordelijkheid en inzet van ons allemaal. We begrijpen dat de omstandigheden tot vragen en bezorgdheid leiden. Als je vragen hebt, stel deze dan aan **<<mij>> <<je manager>>** en zorg goed voor jezelf en je dierbaren.

Het IT team van **<<bedrijf>>**

<<namen / ondertekening>>