



Veilig flexibel, thuis- en telewerken

Beste collega,

Hierbij een aantal aandachtspunten voor het veilig werken.

Let op je omgeving

Wees je ervan bewust dat anderen in je omgeving kunnen meekijken of –luisteren:

1. Werk niet met vertrouwelijke of persoonlijke informatie in openbare plaatsen zoals restaurant, café of in de trein;
2. Let op wie er in de ruimte is wanneer je iets bespreekt of op je scherm bekijkt.
3. Laat je apparatuur niet onbeheerd achter maar houd het bij je.
4. Maak er een gewoonte van om je scherm te vergrendelen wanneer je even weg loopt (Windows toets + L). Doe dit ook op een plek waar je je vertrouwd voelt, zoals thuis.
5. Berg ook thuis je spullen goed op, dus niet bij een raam en zorg dat documenten niet open liggen voor je bezoek of je gezin.
6. Werk niet bij het raam waar anderen van buiten op je scherm kunnen kijken.

Phishing

Cybercriminelen proberen je met chatberichten of e-mail te verleiden om op een link te klikken, informatie te geven of bijvoorbeeld een betaling te doen.

Blijf altijd kritisch nadenken, juist wanneer je onder druk gezet wordt. Twijfel je: pak de telefoon en bel om na te vragen of het wel klopt. Zoek zelf het juiste telefoonnummer op.

Werken met je eigen laptop of smartphone

Heb je een laptop en smartphone van BghU gekregen? Gebruik die dan het liefst.

Werken met je eigen apparaat mag. Houd dan rekening met een paar afspraken:

1. *Zorg dat je apparaat veilig is.*

Veilig betekent:

1. De data ((persoons)gegevens) BghU blijft binnen de interne IT netwerk van de BghU;
2. De laptop (pc) is voorzien van malware/virusscanner en op de volgende wijze geconfigureerd:
 - a. updates worden minimaal 1 x per week bijgewerkt;
 - b. realtime scanning is ingeschakeld;
 - c. minimaal 1x per week worden alle opslag media gescand op malware, en
 - d. alle inkomende e-mail wordt gecontroleerd op virussen;
 - e. de laptop is voorzien van BIT-locker.
 - f. up-to-date software, applicaties, firewall en besturingssysteem inclusief ondersteuning door externe leverancier of it-beheerder;
 - g. toegang tot besturingssysteem is tenminste beschermd door een gebruikersnaam en wachtwoord. Het wachtwoord bestaat uit minimaal:
 - 12 karakters met minimaal (1 hoofdletter, 1 kleine letter, 1 cijfers, 1 vreemd teken(*#^&)).

3. BghU is gemachtigd om steekproefsgewijs te checken dat maatregelen zijn ingericht of een jaarlijkse een verklaring van de externe op te vragen.
4. Alle bedrijfsinformatie van BghU mag niet wordt gebruikt op een draagbare opslagmedium (bijv. USB stick).
5. Gebruik van beveiligd mailen (Zivver) via het netwerk van BghU is verplicht. Het wachtwoord om de mail te openen/document op te halen wordt separaat bijvoorbeeld via mobiel nummer ontvanger verstuurd.
6. Clear Screen en Clean desk wordt door medewerker toegepast:
7. Gevoelige of kritieke bedrijfsinformatie dient achter slot en grendel te worden bewaard, vooral wanneer het kantoor of een spreekkamer verlaten is.
8. Laptop dient te worden afgesloten igv onbeheerd achterblijven of einde werkdag.
9. Hardware is bij tijdelijke) afwezigheid voldoende is beveiligd en/of opgeslagen in een afgesloten ruimte.

2. Informatie niet lokaal opslaan.

Sla geen werkinformatie lokaal op je eigen apparaat op. Daarmee haal je informatie namelijk uit de beveiligde omgeving van BghU. Maak ook geen printscreen van informatie op het scherm.

3. E-mail binnen halen, is ook informatie opslaan.

Gebruik op je eigen apparatuur Outlook. Op je smartphone mag je Outlook installeren uit de App Store of Play Store. Stel niet je @bghu.nl account in op een andere e-mail app.

WIFI buiten kantoor

Om buiten kantoor te werken, moet je soms een onbekend WIFI-netwerk gebruiken. Dat kan redelijk veilig zijn als je op een paar dingen let.

1. Gebruik een betrouwbaar netwerk

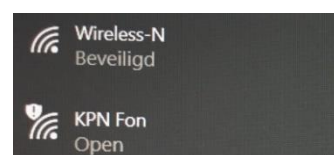
Bijvoorbeeld GovRoam, het WIFI-netwerk van een deelnemer of je beveiligde thuisnetwerk. Verbind alleen met een WIFI-netwerk wanneer je zeker weet dat de naam precies klopt. Vraag na wat de naam moet zijn. Vaak hangt er ook wel een bordje met de naam.

2. Blijf weg van publieke netwerken

Bij de Mc Donalds, in een hotel of op het vliegveld weet je het nooit zeker. Dat geldt voor alle openbare plaatsen. Een kwaadwillende probeert je te verleiden om te verbinden met zijn af luisternetwerk. Hij geeft daarom zijn netwerk een naam die vertrouwen wekt (bijvoorbeeld "Mc Donalds Open WIFI", "KLM Reizigers" of "Van der Valk Gasten"). Sommige WIFI-toegang betaal je uiteindelijk met informatiediefstal.

3. Alleen Beveiligde WIFI

Verbind alleen wanneer een WIFI-netwerk beveiligd is. Op een Open netwerk is het mogelijk om andere gebruikers af te luisteren.



4. *WIFI thuis beveiligen.*

Zet thuis een goed lang wachtwoord op je WIFI-netwerk. Zorg voor een goede, juiste en veilige configuratie. Informeer bij je internetprovider hoe je dat het beste kunt doen. Klik [hier](#) voor een korte video over “Beveiliging tegen cybercriminelen thuis”.

5. *Gebruik de hotspot van je smartphone*

Twijfel je of de WIFI veilig is? Gebruik dan de hotspot van je smartphone die kun je aanzetten via Instellingen > Persoonlijke hotspot. Je telefoon wordt nu een WIFI-toegangspunt voor je laptop of tablet.

Printen

Werk bij voorkeur digitaal. Je hebt dan geen papier met informatie die je moet vernietigen. Heb je toch afdrukken of aantekeningen, gooi deze in de afgesloten blauwe containers op het kantoor van BghU.

Werken met persoonsgegevens

Neem je verantwoordelijkheid.

Vanwege je functie werk je mogelijk met privacygevoelige informatie. Het is niet de bedoeling dat iemand anders dan jijzelf daar toegang tot krijgt. Men kan meeluisteren, – kijken of jouw gebruikersnaam gebruiken om in een systeem te komen. Je bent en blijft altijd verantwoordelijk voor wat er onder jouw naam gebeurt in de systemen van BghU. Neem daarom deze adviezen en richtlijnen serieus en houd je eraan.

1. *Persoonsgegevens niet op je eigen laptop*

Verwerk (gevoelige) persoonsgegevens alleen in de informatiesystemen die daarvoor aangewezen zijn. Volg gemaakte proces- en teamafspraken, en sla geen persoonsgegevens op buiten de informatiesystemen wanneer dat niet noodzakelijk en volgens afspraak is.

2. *Toegang tot gevoelige informatiesystemen en verwerkingen*

Wees terughoudend met vertellen over je rol, verantwoordelijkheden en toegang tot informatie aan personen buiten de organisatie.

- o Spreek hier niet over met anderen.
- o Laat niemand meekijken tijdens het raadplegen van systemen.
- o Geef niemand toegang tot jouw apparatuur

Onderweg

Wanneer je je laptop/tablet, gegevensdrager of papieren meeneemt:

1. *Sluit je laptop altijd af*

Sluit de laptop af op het moment dat je er niet mee werkt. Dus niet in stand-by modus. Een laptop in stand-by is makkelijk te detecteren. Dieven gebruiken hiervoor speciale apparatuur.



Met een laptop die uit staat is dat veel moeilijker.

Bovendien is informatie veiliger wanneer een gestolen laptop uitstaat.

2. *Laat je laptop, gegevensdrager of papieren niet onbeheerd achter*

Ook niet in een afgesloten auto. Ga je een boodschap doen of naar een restaurant, neem de laptop dan mee. Wanneer je papieren meeneemt buiten het kantoor: laat deze niet onbeheerd achter.

Helaas is er niet altijd een veilige oplossing mogelijk. Soms is je laptop of papieren meenemen een groter risico dan deze achter te laten in een afgesloten auto. Probeer dit soort situaties zo veel mogelijk te voorkomen.

Melden van incidenten of datalekken binnen BghU

Meld deze dan direct via Topdesk en mogelijk aan je leidinggevende voor de juiste maatregelen:

1. Ga naar Scientia-portal (homepage);
2. Kies voor de button Topdesk;
3. Inloggen op de Selfserviceportal;
4. Melden (mogelijk) incident of datalek;
5. Vul het formulier zo volledig mogelijk in en voeg eventueel bewijsmateriaal toe.

Incident:

Verwacht jij een verstoring in de dienstverlening van BghU doordat de beschikbaarheid van applicaties wegvalt of dreigt te verminderen. Meld het dan tijdig, binnen 24 uur na bekendwording, want het incident kan impact hebben op:

- De beschikbaarheid van informatie of applicaties voor jou en je collega's, of
- De integriteit (betrouwbaar-, correct- of volledigheid) van informatie komt in het geding of
- Vertrouwelijke informatie komt terecht bij onbevoegde om één of andere reden. In dat geval kan er sprake zijn van een datalek, zijnde:

“is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens”.

Bij twijfel, doe altijd een melding. De collega's van de servicedesk zullen jouw melding bekijken of er werkelijk actie moet worden ondernomen. Zij nemen vervolgens contact op met de privacy officer of de CISO (adviseur op het gebied van informatiebeveiliging).

Vriendelijke dank, want samen houden we BghU veilig.

Marieke Vrisou van Eck
Directeur BghU