simplexxion / stichting VO Haaglanden

ICT Beveiliging
DO's en DON'Ts

wat te doen | wat niet te doen | valkuilen
wat moet u rapporteren | hoe blijft u overtuigend

simplexxion / stichting VO Haaglanden

We zijn gezamenlijk verantwoordelijk voor onze beveiliging. Volg de tips in dit handboek en het zal helpen om uzelf, uw collega’s en ons bedrijf veilig te houden.

Veiligheid geeft ons de vrijheid om te doen waar we goed in zijn. Het is simpel, maar toch essentieel voor uw bedrijf.

Zorg ervoor dat uw familie en vrienden weten hoe ze veilig moeten werken, zodat ook zij veilig zijn op het internet.

1

Laat u niet misleiden door het weggeven van vertrouwelijke informatie

Reageer nooit op e-mails of telefoontjes waarbij er om belangrijke bedrijfsinformatie gevraagd wordt, zoals informatie over medewerkers, financiële resultaten en bedrijfsgeheimen.

Het is makkelijk voor een onbevoegd persoon om ons te bellen en zich voor te doen als een medewerker of een partner.

Blijf altijd waakzaam om dit soort situaties te voorkomen. Mocht u toch verdachte telefoontjes of mailtjes tegenkomen, geef het altijd aan bij onze ICT-verantwoordelijken.

Zorg ook dat u persoonlijke informatie goed beschermt.

2

Gebruik nooit een onbeveiligde computer

Wanneer u gevoelige informatie op een onbeveiligde computer opent, is er een mogelijkheid dat onbevoegde personen de informatie ook kunnen zien. Probeer dit te voorkomen.

Zorg dat u de laatste (goedgekeurde) security patches tot uw beschikking heeft en dat uw antivirus en firewall altijd geüpdatet zijn. Probeer daarnaast altijd in de gebruikersmodus te werken in plaats van de beheerdersmodus.

3

Laat nooit belangrijke informatie achter in uw kantoor.

Zorg ervoor dat u geen uitgeprinte, belangrijke informatie op uw bureau heeft liggen. Belangrijke informatie dient u in een gesloten lade te bewaren of te versnipperen.

Houd uw bureau netjes en berg belangrijke informatie op. Op deze manier ziet uw kantoor er netjes uit en voorkomt u het risico dat belangrijke informatie uitlekt.

4

Vergrendel uw computer en telefoon als u er geen gebruik van maakt

Zorg dat uw computer en telefoon ten allen tijde vergrendeld zijn als u er geen gebruik van maakt. U werkt aan belangrijke documenten, dus is het van belang dat deze documenten beveiligd zijn en dat niemand erbij kan.

Het vergrendelen van uw computer en telefoon zorgt ervoor dat nieuwsgierige mensen niet kunnen meekijken.

5

Blijf alert en rapporteer verdachte activiteiten

Verdachte activiteiten op het internet moet u altijd rapporteren bij onze ICT-verantwoordelijken. Een deel van het werk van onze ICT-partner is om cyberaanvallen tegen te gaan en er voor te zorgen dat er geen documenten zoek raken of gestolen worden.

Al onze functies zijn afhankelijk van het beveiligen van onze informatie. In het geval dat er iets fout gaat, is het van belang dat dit aangegeven wordt. Hoe sneller onze ICT-partner ervan weet, hoe sneller het probleem opgelost kan worden.

6

Bescherm belangrijke informatie en apparaten door middel van een wachtwoord.

U dient er altijd voor te zorgen dat gevoelige informatie op uw computer, USB-stick of smartphone beveiligd zijn met een wachtwoord.

Uw smartphone, USB-stick of laptop verliezen kan altijd gebeuren. Het met een wachtwoord beveiligen van deze apparaten maakt het ongelooflijk moeilijk om in te breken en documenten te stelen.

simplexxion
stichting VO Haaglanden

7

Gebruik altijd moeilijk te raden wachtwoorden

Gebruik geen makkelijke wachtwoorden zoals “kat” of een makkelijke cijfercombinatie zoals “12345”. Het is beter om een ingewikkeld wachtwoord te hebben met hoofdletters, nummers en interpunctie.

Probeer verschillende wachtwoorden voor verschillende websites te hanteren zodat als er één gehackt wordt, de anderen nog goed beveiligd zijn.

*$e7enal1ig@t0r5inmyb^th
(seven alligators in my bath)

8

Wees voorzichtig met verdachte e-mails of links

Laat uw nieuwsgierigheid u niet fataal worden.

Verwijder ten allen tijde verdachte e-mails of links. Zelfs het openen of het bekijken van deze e-mails en links kan vervelende gevolgen hebben zonder dat u het door heeft.

Onthoud: als iets te mooi lijkt om waar te zijn, is dat het waarschijnlijk ook.

9

Plug nooit persoonlijke apparaten in de apparaten van uw bedrijf zonder toestemming van de ICT-verantwoordelijke

Plug nooit persoonlijke apparaten zoals een USB-stick of uw smartphone in een computer zonder toestemming van de ICT-verantwoordelijke.

Deze kunnen worden aangetast op het moment dat u hem aansluit op de computer.

Bespreek het eerst met de ICT-verantwoordelijke voordat u uw persoonlijke apparaat aansluit op uw werk.

10

Installeer nooit onbevoegde programma’s op uw werkcomputer

Kwaadaardige programma’s lijken er vaak betrouwbaar uit te zien, zoals games, apps en zelfs antivirussoftware.

Ze zijn bedoeld om je in de maling te nemen en het zorgt voor virussen op uw computer of netwerk.

Als u een applicatie tegenkomt die u wilt gebruiken, neem eerst contact op met uw ICT-verantwoordelijke voordat u de applicatie installeert.

Voortdurende inspanning

Zolang computers zullen bestaan zullen de bedreigingen hiervan ook blijven bestaan. Deze top 10-lijst zal naarmate de tijd vordert steeds aangepast moeten worden, omdat er altijd nieuwe bedreigingen ontstaan.

Houd de updates van dit handboek in de gaten, zodat uzelf en ons bedrijf niet in gevaar zullen komen.

© Simplexxion

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enkele wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige manier, zonder voorafgaande toestemming van de uitgever. Voor het overnemen van gedeelte(n) uit deze uitgave n lezingen, readers en andere compilatie- of andere werken (artikel 16, Auteurswet 11212), in welke vorm dan ook, dient men zich tot de samenstellers/uitgever te wenden.