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

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 of leerlingen, financiële resultaten of bedrijfsgeheimen.

Het is makkelijk voor een onbevoegd persoon om ons te bellen en zich voor te doen als een medewerker of een partner. Gebeurd dit en vertrouwd u het niet, noteer de gegevens en vertel dat u het uitzoekt en hier later op terug komt, overleg desnoods met u leidinggevende.

Blijf altijd waakzaam om dit soort situaties te voorkomen. Mocht u toch verdachte telefoontjes of mailtjes tegenkomen, geef dit direct door aan de ICT afdeling.

Zorg dat u uw persoonlijke informatie goed beschermt en gebruik voor werk geralateerde zaken altijd het email adres van de school, gebruik nooit privé e-mailaccounts.

2. Gebruik nooit een onbeveiligde computer

Gebruik alleen een computer die gebruik maakt van de laatste security patches en welke beschikt over een antivirus programma en een firewall, deze moeten up-to-date zijn. Probeer daarnaast altijd in de gebruikersmodus te werken in plaats van de beheerdersmodus.

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.

De school computers zijn beveiligd maar let altijd op met verdachte mails en verwijzingen naar links en update ook uw privé computer thuis regelmatig.

3. Laat nooit belangrijke informatie achter in uw kantoor

Zorg ervoor dat u geen uitgeprinte, belangrijke informatie op uw bureau laat liggen. Belangrijke informatie dient u in een gesloten lade te bewaren of te versnipperen. Hieronder verstaan we ook informatie met betrekking tot de privacy wetgeving, zoals persoonsgegevens.

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 smartphone als u er geen gebruik van maakt

Zorg dat uw computer en smartphone ten allen tijde vergrendeld zijn als u er geen gebruik van maakt. Ook als dit maar voor 5 minuten is. Meldt u zich netjes af als u niet meer terug komt op de werkplek zodat de computer netjes afgesloten wordt.

Hoe kunt u dit doen?

Toets op de computer "Ctrl+Alt+Del" en kies voor "Vergrendelen".

U heeft toegang tot belangrijke documenten op het netwerk, het is dus van belang dat deze documenten veilig zijn en dat niemand hier mbv uw account bij kan als u van uw werkplek weg bent.

Vergrendel ook altijd uw(prive) smartphone. Zorg er altijd voor dat u een pincode / veegpatroon of een wachtwoord moet invoeren voor dat u de smartphone kunt gebruiken. Hoe stelt u dit in ? U kijkt onder instellingen en zoekt hier naar schermvergrendeling of beveiliging. Waarom ? Om misbruik te voorkomen en ervoor te zorgen dat bij diefstal uw gegevens niet op straat liggen. Hier geldt dan ook hoe complexer, hoe moeilijker deze is te openen voor een ander.

Het vergrendelen van uw computer en smartphone zorgt ervoor dat :

- nieuwsgierige mensen niet kunnen meekijken
- er geen misbruik van u gegevens gemaakt kan worden

5. Blijf alert en rapporteer verdachte activiteiten

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

Ook in het geval dat er iets fout gaat op of met de computer, is het van belang dat dit aangegeven wordt. Hoe sneller onze ICT afdeling ervan weet, hoe sneller het probleem opgelost kan worden en de risico's bekeken kunnen worden.

Ook in het geval van schade, vermissing of diefstal van ICT- middelen dient de ICT afdeling z.s.m. op de hoogte gebracht te worden zodat zij de juiste vervolgstappen kunnen nemen.

6. Bescherm belangrijke informatie en apparaten door middel van een wachtwoord of token

U dient er altijd voor te zorgen dat gevoelige informatie op uw computer, USB-stick of smartphone beveiligd zijn d.m.v. een wachtwoord of beter nog d.m.v. een wachtwoord en MFA.

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. Bij verlies van een smartphone, USB-stick of laptop, neemt u altijd contact op met onze ICT- verantwoordelijke.

Multi-Factor authentication (via een App of hardware token) wordt gebruikt als extra beveiligingsmiddel. Voor een belangrijke applicatie zoals Magister wordt er al gebruik gemaakt van MFA. Een kwaadwillende heeft dan niets aan alleen uw inlognaam en wachtwoord maar heeft dan ook nog een token nodig om in te kunnen loggen
Wees zuinig op uw hardware token, laat deze niet rondslingeren en bij verlies moet u dit direct melden aan de applicatiebeheerder of de ICT afdeling.

7. Gebruik altijd moeilijk te raden wachtwoorden

Gebruik verschillende wachtwoorden voor verschillende websites, als er één gehackt wordt, zijn de anderen nog goed beveiligd. Maak een wachtwoord niet te makkelijk zoals “kat” of een makkelijke cijfercombinatie zoals “12345” en maak waar mogelijk gebruik van Multi-Factor authenitcatie. Het is beter om een ingewikkeld wachtwoord te hebben met hoofdletters, nummers en interpunctie. Gebruik ook voor uw prive accounts "veilige" wachtwoorden.

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

Laat wachtwoorden niet rond slingeren. (gebruik ook geen post-it op uw monitor of een kladblok naast uw pc of onder uw keyboard) Maak evenuteel gebruik van een wachtwoorden kluis maar alleen in overleg met uw ICT medewerker.

Bijvoorbeeld: *https://www.lastpass.com/*

Hierin kunt u verschillende wachtwoorden in een beveiligde omgeving bijhouden.

Deel u wachtwoord **nooit** met iemand. Er zijn vaak andere oplossingen voor het feit dat uw collega niet bij een mail of bestand kan komen op het moment dat u niet aanwezig bent. Vraag naar de mogelijkheden aan uw ICT afdeling.

Laat in geen enkel geval iemand anders gebruik maken van uw persoonlijke inloggevens.

Bedrijven zullen iig nooit telefonisch om uw wachtwoord vragen. Om een wachtwoord te resetten hebben zij genoeg aan uw inlognaam en/of e-mail adres.

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. Het openen of het bekijken van deze e-mails en links kan vervelende gevolgen hebben zonder dat u het door heeft.

Let goed op nep facturen in uw mailbox, controleer altijd het e-mail adres waar het bericht vandaan komt. Hierin zie je meestel snel genoeg dat het niet juist is omdat het email adres geen officieel adres van het betreffende bedrijf is.

Twijfel je nog steeds ? Neem in dat geval contact op met de ICT afdeling of kijk op deze site :
https://www.fraudehelpdesk.nl/sub-vragen/phishingmails/

Onthoud:
Als iets te mooi lijkt om waar te zijn, is dat waarschijnlijk ook zo!!!

9. Plug nooit persoonlijke apparaten in de apparaten van uw school

Plug nooit persoonlijke apparaten zoals een USB-stick of uw smartphone in een computer op school zonder toestemming van de ICT-verantwoordelijke. Uw persoonlijke apparaten kunnen hierdoor worden aangetast op het moment dat u hem aansluit op de computer bv als de encryptie geforceerd wordt. Andersom kunnen we virussen vanaf uw prive computers op het schoolnetwerk terecht komen.

Bespreek altijd eerst met de ICT afdeling wat u van plan bent voordat u uw persoonlijke apparaat aansluit op het schoolnetwerk of een school apparaat.

We adviseren u ook om een sterk wachtwoord en/of pincode op al uw persoonlijke apparaten in te stellen.

10. Installeer zelf geen software op uw schoolcomputer

Kwaadaardige software ziet er soms heel betrouwbaar uit, de software wordt aangeboden als gams, app of zelfs als antivirussoftware. De software is echter gemaakt om u in de maling te nemen en het zorgen voor risico's voor virussen op uw computer of netwerk en daarom moet de software eerst gecontroleerd worden.

Software die op school gebruikt wordt moet vanzelfsprekend ook legaal zijn, ofwel er moet een licentie voor worden aangeschaft. De ICT afdeling zorgt er ook voor dat de juiste licenties aangeschaft worden.

Het is om bovenstaande redenen dan ook niet toegestaan om zonder toestemming van het systeembeheer zelf software op een schoolcomputer/laptop te installeren of om daartoe een poging te doen. Als u een applicatie tegenkomt die u wilt gebruiken, moet u eerst contact opnemen met de ICT afdeling. Installaties van software op apparaten van school worden altijd uitgevoerd door de ICT afdeling.

Wees alert - laat u nieuwsgierigheid, u niet fataal worden — Te mooi om waar te zijn — Bij twijfel niet openen

Mail

Let op !

Let op !
Blijf alert en rapporteer verdachte activiteiten. Laat u niet misleiden. Reageer niet als men om belangrijke bedrijfsinformatie vraagt of informatie van medewerkers en leerlingen. Meld dit direct.

Onbeheerde papieren

Berg belangrijke informatie altijd goed op. Op deze manier voorkomt u het risico dat belangrijke informatie uitlekt.

Vergrendelen

Even koffie halen of naar de wc ?
Vergrendel uw apparaten. Het onbeheerd achterlaten van (gevoelige) informatie kan in enkele minuten leiden tot een datalek.

Wachtwoord

Zorg ervoor dat gevoelige informatie op uw computer, USBstick of smartphone beveiligd zijn met een wachtwoord. Moeilijk te raden wachtwoord. Verschillende wachtwoorden.

Beveiligde apparaten

Een beveiligde computer maakt gebruik van de laatste (goedgekeurde) security patches, heeft een up to date virusscanner en firewall. Controleer dit bij niet school gerelateerde apparaten.

Geautoriseerde programma's

Neem contact op met uw ICT verantwoordelijke

Privé apparaten

Bespreek het eerst met de ICT-verantwoordelijke voordat u uw persoonlijke apparaat aansluit op uw werk. (smartphone of USBstick etc.)