Informatiebeveiliging & privacy goed geregeld!

Deel 7: Hoe blijf je veilig online?

De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 7: veilig online.

Klik op het puzzelstukje voor een korte introductie!

Veilig online - wat betekent dat?

Iedereen is via allerlei devices, steeds meer online. Daar zitten veel voordelen aan: je beschikt op elk moment snel over informatie vanaf elk device. Maar er kleven ook nadelen aan. Let daarom goed op wat je online doet, vooral wanneer je privé en werk combineert op dezelfde devices.

Wil je een app gebruiken, dan moet je meestal inloggen met een gebruikersnaam of e-mailadres met een wachtwoord. Op websites moet je cookies accepteren. Zo laat je een online voetafdruk met veel (persoonlijke) informatie achter. En die gegevens zijn geld waard.

Meer weten over hoe een online voetafdruk werkt? Bekijk filmfragment van 'Dave, een fantastische waarzegger.'

Persoonsgegevens online delen

Als je persoons gegevens (online) deelt met anderen, dan moet je erop kunnen vertrouwen dat de ontvanger er zorgvuldig mee om gaat. Ook ouders verwachten dat wij als medewerkers van <naam schoolbestuur> zorgvuldig omgaan met de persoonsgegevens van hun kinderen. Hiervoor heb je kennis en vaardigheden nodig om met de digitale wereld om te gaan.

Onbeveiligde netwerken

Best gemakkelijk dat je wifi hebt zonder dat je hoeft in te loggen? Dat is dus een onbeveiligd netwerk. Voor hackers wordt het zo heel eenvoudig om je smartphone, tablet of computer voor de gek te houden. Met speciale apparatuur kan een netwerk aangemaakt worden met de naam van het openbare wifi-netwerk (zoals de bibliotheek, een café of de trein) waar je apparaat vervolgens verbinding mee maakt. Hierna kan een hacker meekijken met wat je doet of gegevens stelen, zoals werkgegevens van de school. Vermijd daarom gratis openbare wifi-netwerken.

Klik niet klakkeloos

Heb je ooit een Phishing mail gehad?

Phishing (afgeleid van vissen en hengelen) is een vorm van internetfraude. Je wordt, via bijvoorbeeld een link in een mailtje, naar een valse website gelokt met bijvoorbeeld het verzoek om je inloggegevens te controleren. Als je hier – nietsvermoedend – je inlognaam en wachtwoord of je creditcardnummer invult, krijgt de fraudeur achter de schermen de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij vaak voor als een vertrouwde instantie of persoon, zoals een bank, het postkantoor of zelfs een familielid.

Wat zijn cookies eigenlijk?

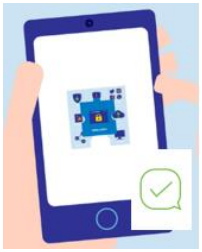
Een cookie is een tekstbestandje dat door een server op uw computer, smartphone of tablet kan worden geplaatst. Cookies onthouden dat je bent ingelogd op een site, welke artikelen er in je winkelmandje zitten, je voorkeursinstellingen en worden gebruikt voor statistieken.

Dat kan handig zijn, maar wil je het altijd? Daarvoor is er de cookiewet die eist dat je duidelijk geïnformeerd wordt en expliciet toestemming moet geven voor NIET-noodzakelijke cookies, die jouw privacy kunnen schenden. De beslissing is aan jou.

Hoe veilig ben jij online?

Weet jij waar malware vandaan komt? En of je automatische updates op je pc altijd moet goedkeuren? Doe de zelf-check via Nederland Veilig Online!

Als je zelf de valkuilen kent en hoe je daarmee om moet gaan, dan kun je ook leerlingen helpen 'online bekwaam' te worden.



Als medewerkers van CSW vraagt dit van ons dat we weten:

- welke risico's er online zijn en dat we terughoudend moeten zijn met het online plaatsen van (persoons)gegevens (niet alleen op school, maar ook thuis).
- wat de gevolgen kunnen zijn van het gebruik van openbare wifi-netwerken.
- wat malware en phishing zijn en hoe we het kunnen herkennen.
- welke maatregelen we zelf kunnen nemen om veilig online te zijn.

Sleutelwoorden deel 7: online gegevens, cookies, onbeveiligde netwerken, openbare netwerken, malware, phishing

De serie IBP-berichten is mogelijk gemaakt door Kennisnet