DEEL 2

Hoe blijft u veilig online?

Beste ouders/verzorgers,

De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kunt er eigenlijk mee? In negen IBP-berichten met animatiefilmpjes bent u helemaal up-to-date! In deel 2: veilig online.

Veilig online - wat betekent dat?

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

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

Persoonsgegevens online delen

Als u persoons gegevens (online) deelt met anderen, dan moet u erop kunnen vertrouwen dat de ontvanger er zorgvuldig mee om gaat. Van ons als medewerkers van Onderwijsgroep GAVE mag u verwachten dat wij zorgvuldig omgaan met de persoonsgegevens van u en uw kinderen. Hiervoor hebben wij ook kennis en vaardigheden nodig, om met de digitale wereld om te gaan.

Onbeveiligde netwerken

Best gemakkelijk dat u wifi hebt zonder dat u hoeft in te loggen? Dat is dus een onbeveiligd netwerk. Voor hackers wordt het zo heel eenvoudig om uw 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 uw apparaat vervolgens verbinding mee maakt. Hierna kan een hacker meekijken met wat u doet of gegevens stelen, zoals bijvoorbeeld betalingsgegevens. Vermijd daarom gratis openbare wifi-netwerken en doe op beveiligde openbare netwerken geen belangrijke zaken zoals bankieren (of gebruik een VPN)

Klik niet klakkeloos

Heeft u ooit een Phishing mail gehad? Phishing (afgeleid van vissen en hengelen) is een vorm van internetfraude. U wordt, via bijvoorbeeld een link in een mailtje, naar een valse website gelokt met bijvoorbeeld het verzoek om uw inloggegevens te controleren. Als u hier – nietsvermoedend – uw inlognaam en wachtwoord of uw 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. Tevens bestaat het risico dat u door het klikken op de link maleware op uw computer binnenhaalt.

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 u bent ingelogd op een site, welke artikelen er in uw winkelmandje zitten, uw voorkeursinstellingen en worden gebruikt voor statistieken.

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

Wilt u meer lezen over mediawijsheid? Kijk dan op de website van www.mediawijsheid.nl

Mediawijsheid.nl
De betrouwbare wegwijzer in veilig en slim gebruik van (digitale) media

De volgende keer:

Wat doet Onderwijsgroep GAVE op het gebied AVG en IBP?

onderwijsgroep gave

De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad