# **5 terug-naar-school tips om kinderen te helpen veilig online te blijven**

Nu de vakantie bijna is afgelopen en veel kinderen terug naar school moeten, zullen ze het internet en hun smartphones gebruiken voor schoolwerk en om af te spreken. Uiteraard vindt Sophos het belangrijk dat kinderen veilig en verstandig tewerk gaan wanneer zij zich online bevinden. Daarom deelt de marktleider voor de volledige IT-beveilinging graag deze top-5 terug-naar-school tips.

Tip voor de ouders: indien de kinderen nog niet bekend zouden zijn met deze tips, neem dan even de tijd om ze samen door te nemen, zodat ze een uitstekende online belevenis hebben dit schooljaar.

**1) Indien je het niet persoonlijk zou delen, doe dat dan ook niet online**

Veel zaken die online worden gedeeld, lijken alsof dat delen enkel gebeurt tussen twee partijen. Maar het is wel degelijk zo dat publieke berichten (of berichten die publiek worden gedeeld) door iedereen kunnen worden gelezen.

Zaken die je online post kunnen ook een lang leven hebben. Dus als je niet wil dat de ganse wereld (inclusief je oma) bepaalde zaken leest of ziet omdat ze te beschamend of persoonlijk zijn, post ze dan niet! Zelfs niet als de app aangeeft dat bepaalde posts vervallen, zijn er altijd manieren om daar een mouw aan te passen.

Ten laatste, vergeet niet dat je posts of woorden een bepaalde kracht hebben, zelfs online. Een goede online burger weet dat wat je ook over anderen zegt, een diepe impact kunnen hebben. Dus wees vooral vriendelijk en onthoud, als je niet wil dat een ander op een bepaalde manier over jou praat, dan moet je dat zelf ook niet doen.

**2) Hou je posts privé en beperk je profiel tot het minimum**

Heb je de privacy van je sociale media profielen al nagekeken? Hier komen enkele tips om je Facebook- en Instagram-profielen te vergrendelen.

Over het algemeen is het een goed idee om je profiel enkel open te zetten voor vrienden zodat je precies kan nagaan wie je posts kan zien. Er zijn ook vele privacy opties per sociaal netwerk. Dus het is goed om altijd je eigen privacy instellingen in het oog te houden en die van tijd tot tijd na te kijken.

Onthoud dat wat je ook privé post, je nooit de volledige garantie hebt dat die informatie veilig is opgeslagen. Men zou bijvoorbeeld een screenshot kunnen nemen en delen? Wees ook karig met de informatie die je deelt, zoals je adres, locatie, e-mailadres of persoonlijke informatie, want al die informatie is toegankelijk voor iedereen. En je wil niet dat iedereen over die informatie beschikt, natuurlijk.

**3) Delen is lief, maar niet wanneer het over paswoorden gaat**

Paswoorden zouden uniek moeten zijn, en persoonlijk.

Het is natuurlijk een stuk gemakkelijker om hetzelfde paswoord voor al je apps en websites te hebben. In de realiteit is het zo dat indien iemand je e-mailadres en paswoord kent voor slechts één website, ze nu toegang hebben tot alles.

Dit gebeurt namelijk vaak wanneer sites worden gehackt. Hackers gaan er prat op dat mensen hun paswoorden hergebruiken en eenmaal ze een site hebben gehackt, proberen ze die paswoorden op andere sites.

Het is ook niet verstandig om accounts en paswoorden met vrienden te delen. Indien je een account deelt met een vriend, en zijn of haar telefoon wordt gestolen of gehackt, komen ook al jouw accounts in gevaar. De oplossing is gemakkelijk: deel geen accounts!

**4) Wees een voorzichtige downloader**

Wanneer je aan je telefoon of computer denkt zoals aan je eigen lichaam, dan zou je ook niet eender welk voedsel opeten dat je op straat hebt gevonden. Daarom moet je ook voorzichtig zijn met spullen die je op je toestellen zet. Niet te vertrouwen apps of programma’s kunnen je telefoon of computer ernstig beschadigen, en in sommige gevallen persoonlijke informatie te grabbel gooien.

Wees dus voorzichtig waarop je klikt, of het nu een link is naar een leuk uitziende e-mail, een vragenlijst of leuke en gratis software. De meest veilige manier is om apps van de officiële app stores te downloaden voor je telefoon, en niet van eender welke website.

**5) Log uit en sluit af**

Wanneer je niet langer een app of website gebruikt, zorg er dan voor dat je bent uitgelogd. Dit is vooral belangrijk wanneer je een publieke computer gebruikt op school of in de bibliotheek, of zelfs in een winkel. Zoniet geef je de volgende persoon vrije toegang tot jouw Facebook-account en persoonlijke e-mails.

Het is ook verstandig om een paswoord voor je telefoon te gebruiken. Ook al lijkt dit nogal ongemakkelijk, de voordelen wegen zeker op tegen de nadelen.

Zou hou je al je apps en accountinformatie uit de handen van een dief, indien je ooit toegang tot je telefoon zou verliezen. Het voorkomt ook dat je vrienden grapjes kunnen uithalen, als ze ooit je telefoon kunnen bemachtigen.

Een paswoord is een super simpele, maar zeer efficiënte manier om te verhinderen dat anderen in jouw naam posten, of zelfs spullen via jouw account aankopen. Zoiets simpel als een paswoord kan helpen om heel veel (voorkombare) problemen te vermijden.

**Heb je zelf tips voor ons?**

Hoe zit het met jou? Heb je zelf tips die je met ons wil delen om kinderen te helpen veilig online te zijn? Dan horen we die graag.