kids week IN DE KLAS
WERELD & TAAL

Hallo internet, dag privacy

Je kunt chatten met je vrienden, waar jullie ook zijn. Informatie vind je in een handomdraai. En als je je verveelt ga je toch een potje gamen? Internet maakt ons leven een stuk makkelijker. Maar we leveren er wel onze privacy voor in. Hoe dan? En wat kun je ertegen doen?

PESTEN IS ZO GEPIEPT

Iemand pesten is door het internet wel heel makkelijk geworden. Met één druk op de knop zet je een gemene roddel online, of scheld je iemand uit. Dat is niet alleen naar omdat je door veel mensen tegelijk gepest kan worden, maar ook omdat foto's en berichtjes moeilijk van het internet te halen zijn.

VIRUSSEN, HACKERS EN ANDERE GRIEZELS

Hackers proberen gegevens van anderen te achterhalen. Bijvoorbeeld met nepmails waarin ze om informatie vragen, of waarin een virus verstopt zit. Zo'n virus kan wachtwoorden of bestanden stelen, lezen wat je typt, of je computer overnemen. En dan zijn er ook nog mensen die zich voordoen als een ander, bijvoorbeeld een kind, of een modellenbureau. Zo proberen ze contact met kinderen te leggen. En meestal niet met de beste bedoelingen!

SPOREN IN DE UITVERKOOP

Wist je dat je online overal sporen achterlaat? Als je een site bezoekt zet die cookies op je computer. Cookies verzamelen informatie over jou. Ze weten welke websites je bekijkt en wat je daar invult. Dankzij cookies weten bedrijven wat jij online uitspookt. Die kennis verkopen ze weer door aan andere bedrijven, die jou steeds beter kennen. Ze sturen je precies de advertenties waar jij gevoelig voor bent. En dat met maar één doel: ze willen geld aan je verdienen.

WEG CONTROLE

Berichten en foto's worden online vaak snel gedeeld en verspreid. Als iets online staat, heb je er dus geen controle meer over. En je krijgt het ook niet zomaar weg. Dat kan jaren later nog nare gevolgen hebben, als je gaat solliciteren bijvoorbeeld.

MAIL VAN KLOOP

Hoi, er is iets mis met je bankpas. Mag ik je pincode? Groetjes, ~~Scoop~~ Kloop



PANIEK, OF GEEN PANIEK?

Tja, wat nu? Moet je je social media-accounts wissen en je computer uit het raam gooien? Natuurlijk niet! Het helpt al als je de online gevaren kent en weet wat je kunt doen. Dat lukt nog beter met deze tips.

- Vraag je, voordat je iets online zet, altijd dit af: wie kan deze informatie zien en wat mag diegene van mij weten? Kan iemand dit gebruiken om mij (later) te kwetsen? Zou ik boos zijn als iemand dit met anderen deelt? Wat is het ergste dat kan gebeuren als ik dit deel?
- Verzin wachtwoorden van minstens acht tekens, waaronder cijfers, letters en speciale tekens. Geef ieder account een ander wachtwoord.
- Gebruik geen openbare WiFi-netwerken. Die zijn niet veilig.
- Open geen mails van onbekenden en geef nooit je wachtwoord, foto's of andere informatie.
- Check je privacy-instellingen op social media. Wie kan lezen wat jij post? Scherm je profiel af voor onbekenden. Bij Instagram doe je dat bij 'instellingen'. Daar klik je op 'privacy'.
- Accepteer niet iedereen als vriend.
- Vraag het eerst voordat je iemand tagt.



WIST JE DAT...

- je niet alle informatie te zien krijgt als je via Google zoekt? Google let op je eerdere zoekgedrag en resultaten. Andere resultaten worden genegeerd.
- je anoniem kunt zoeken via de website Startpage.com? Hetzelfde geldt voor de zoekmachine DuckDuckGo.com.
- je een veilige website kunt herkennen aan 'https' in de adresbalk? Vaak zie je ook een icoon van een slotje.
- Instagram, Snapchat, Facebook en Twitter een helpcentrum hebben? Daarin staan tips voor privacy & veiligheid. Je kunt bijvoorbeeld vinden hoe je volgers kunt verwijderen, hoe je je account op privé zet en hoe je iemand blokkeert.
- ook Snapchat al jouw foto's, stem en chats opslaat en aan bedrijven verkoopt? Snapchat verdient veel geld aan jou. Bepaal zelf wat je deelt bij 'instellingen'. Op de site van de Consumentenbond vind je meer tips.

Andere handige sites zijn mediawijsheid.nl en veiliginternetten.nl

