Achtergrondinformatie – Hacken, AI en toch veilig online?

Hacken

'Hacken' betekent oorspronkelijk: een creatieve oplossing voor een technisch probleem. Dat is het eigenlijk ook. Een hacker loopt tegen een probleem aan en moet een oplossing verzinnen om weer een stap verder te komen. Hiervoor heeft hij allerlei kennis, vaardigheden en technieken nodig. Hacken in de oorspronkelijke betekenis van het woord zorgt er dus voor dat je beter weet hoe computers werken, wat ze kunnen en wat niet.

Inmiddels heeft hacken ook een hele andere betekenis gekregen. Hacken betekent tegenwoordig meestal ongeoorloofd een computer, tablet, telefoon of een softwareplatform binnenkomen, of een wachtwoord ontfutselen met nepberichten over bijvoorbeeld je bankrekening (phishing) of via gevaarlijke bijlagen in een e-mail. Wanneer je zo'n bijlage opent, kan een hacker je computer overnemen of er virussen op installeren. Dat laatste kan ook via downloads en links (malware) of online advertenties. Uiteraard is deze vorm van hacken ongeoorloofd en strafbaar.

Soorten hackers

Er zijn twee soorten hackers: de 'white hat hackers' en de 'black hat hackers'. De 'white hat hackers', ook wel ethische hackers genoemd, speuren kwetsbaarheden op, zorgen ervoor dat die weer gedicht worden of laten de bouwer weten welke kwetsbaarheden ze gevonden hebben. White hat hackers maken het internet op deze manier een beetje veiliger. Maar 'black hat hackers' hebben kwade bedoelingen. Ze willen inbreken in je computer om je in de gaten te houden, gevoelige informatie te vinden (zoals wachtwoorden, paspoortgegevens, vingerafdrukken of naaktfoto's) of geld te stelen.

Een tussenvorm zijn 'hacktivisten'. Dit zijn hackers die hacken voor 'de goede zaak', zoals voor een politieke zaak of een milieukwesties. Het kan ook zijn dat hij of zij gemakkelijk of gratis toegang tot besloten informatie, diensten of producten wil geven uit een rechtvaardigheidsgevoel, waarbij in de ogen van de hacktivist het doel het middel heiligt.

Hacken met AI

Kunstmatige intelligentie, AI, maakt het voor hackers gemakkelijker om te hacken. Met AI kunnen gemakkelijk nepfoto's en nepberichten worden gemaakt. Programma's als ChatGPT maken overtuigende teksten zonder de (spel-)fouten die hackers zelf vaak wel maken. Dat maakt het

moeilijker om kwaadwillende appjes en e-mails te herkennen. Bovendien kunnen hackers met AI sneller wachtwoorden raden of een nepbeeld van iemands gezicht maken.

Betaalde content openbaar maken

Het is ook strafbaar om anderen te laten meeliften op jouw account voor een betaalde muziek- of streamingdienst. Ook dat is feitelijk een vorm van hacken. Het is nadelig voor de makers die daardoor de vergoeding voor het gebruik mislopen. En uiteindelijk nadelig voor ons allemaal, omdat er dan minder geïnvesteerd kan worden in makers en diensten om nieuwe content te maken en aan te bieden.

Heel vervelend is het ook als een website of account gehackt wordt waar jouw eigen werk op staat, zoals jouw berichten en foto's die je alleen met jouw vrienden wilt delen.
Die kunnen dan gedeeld worden. Daarvoor heb jij als rechthebbende geen toestemming gegeven en jouw werk of jij persoonlijk kan daardoor ook in een verkeerd daglicht worden gezet. Het auteursrecht op jouw foto's, filmpjes of teksten beschermt jou tegen het verspreiden van jouw werk zonder jouw toestemming.

Online veiligheid vergroten

Hoe kun je je persoonlijke gegevens en je online werk beveiligen? Met deze tips wordt het voor hackers moeilijker om bij jou binnen te komen:

1. Gebruik een sterk wachtwoord (minimaal 12 karakters en een combinatie van letters, symbolen, hoofdletters en kleine letters) en gebruik voor iedere toegang een ander wachtwoord;
2. Vernieuw je wachtwoorden regelmatig (bijvoorbeeld 1 keer per jaar of nadat je ergens 10 keer hebt ingelogd);
3. Gebruik een wachtwoordkluis, zodat je overal een ander en sterk wachtwoord voor kunt gebruiken en je ze niet allemaal hoeft te onthouden;
4. Gebruik zo min mogelijk openbare wifi;
5. Koppel zo min mogelijk accounts aan elkaar;
6. Installeer software-updates zo snel mogelijk;
7. Zorg dat je regelmatig een back-up maakt;
8. Gebruik een veilige browser;
9. Beveilig zeer gevoelige gegevens met tweestapsverificatie, bijvoorbeeld een wachtwoord en daarna nog een code die je via je telefoon ontvangt;
10. Klik niet zomaar op linkjes of e-mailbijlagen; pas ook op dat je daartoe niet verleidt wordt met gratis aangeboden content.
11. Gebruik, bijvoorbeeld op je telefoon, een vingerafdrukscan.
12. Wees sceptisch over berichtjes van nummers die je niet kent, ook al lijkt het een persoon die je kent. Geef nooit zomaar je gegevens als je het niet vertrouwt en maak nooit zomaar geld over.

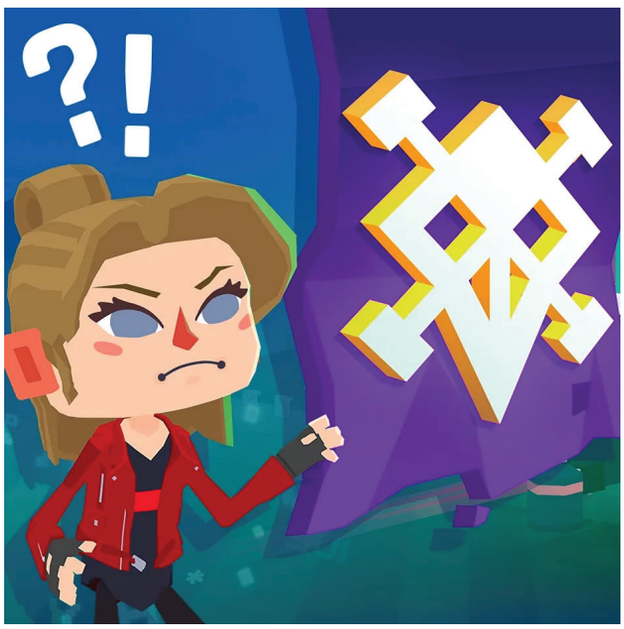
Tips voor de leerkracht voor een volgende keer

- Korte les Foto's delen: Deze korte les gaat over het bewust omgaan met foto's waar anderen op staan.
- Verdiepingsles Portretrecht: Wanneer iemand iets vervelends doet met een foto waar jij op staat, heb jij jouw portretrecht om daar bezwaar tegen te maken.
- Verdiepingsles Welke rechten heb ik als maker?: In deze les leren de kinderen dat zij heel vaak ook zelf maker zijn en dus auteursrecht hebben.

Er zijn drie verdiepingslessen die bestaan uit een introductievideo van Tobias, een op leesniveau groep 7/8 gemaakte leestekst over respectievelijk de rechten van een gebruiker, de rechten van een maker en een over portretrecht, waarna de leerlingen in een quiz hun in de leestekst opgedane kennis kunnen toetsen. Daarnaast is er nog een leuke doe-opdracht in de vorm van een woordzoeker, kruiswoordpuzzel of discussievragen. Zeker als er al een korte les met de klas is gegeven over één van deze thema's, lenen de verdiepingslessen of onderdelen daaruit zich ook voor zelfstandig werken.

Copy Koppie Quest

Een leuke en leerzame aanvulling en combinatie met het lespakket Wijs met media omgaan is de game die in en met de klas kan worden gespeeld: de Copy Koppie quest.



In deze klassenquest, onderdeel van het populaire programma HackShield, leren de kinderen dat als zij maker zijn van originele werken, zij en hun werk door het auteursrecht worden beschermd. Ze leren ook wanneer je werk van een ander wel en niet mag gebruiken. Leerlingen staan bovendien stil bij het gebruiken, plaatsen of verkopen van afbeeldingen van anderen. Mag je een afbeelding die je via Google vindt vrij gebruiken? En mag je deze afbeelding zomaar verkopen? In de Quest helpen de leerlingen Papi het goede pad op. De quest is voorzien van een lesbrief.

Op de HackShield website kun je alle informatie over de Copy Koppie klassenquest vinden, inclusief de lesbrief en het aanmaken van een leerkrachtaccount.

Meer informatie over auteursrecht?

Wil je meer weten over auteursrecht? Dan kun je terecht op de volgende websites:

- auteursrechtvoorjou.nl: algemene informatie over auteursrecht geschikt voor kinderen. Met het informatiefilmpje 'Auteursrecht in twee minuten'.
- onderwijsenauteursrecht.nl: speciaal voor leerkrachten, over het gebruik van auteursrechtelijk beschermd materiaal in het onderwijs. Hier kan je snel vinden welke regelingen er zijn getroffen voor gebruik in het onderwijs.
- auteursrecht.nl: voor algemene informatie over het auteursrecht.