Handleiding - Digitale Hygiëne

Deze handleiding bevat de ‘theorie’ achter de workshop Digitale Hygiëne.

[Slide 5]
Klasvraag: Wat is hacken?

- Geef studenten de mogelijkheid om te vertellen wat ze denken dat hacken is.
- Geef een samenvatting van de antwoorden die door de leerlingen worden gegeven. Soms zijn het lange, warrige verhalen, dan is het fijn als de hele klas weet wat er gezegd werd door de samenvatting.

Veel voorkomende antwoorden:

- Het hacken van iemands wachtwoord
- Stelen van bankgegevens
- Inbreken op de computers van crimenelen of boeven.

Soms antwoorden:

- De wereld veiliger maken door op zoek te gaan naar kwetsbaarheden in websites

[Slide 6] Leg nu uit wat hacken precies is.

Er is verschil tussen goed hacken en slecht hacken. Slecht hacken is crimineel hacken, ookwel cracken genoemd. Dit is bijvoorbeeld het stelen van bankgegevens van je vader of moeder, of het hacken van iemand zijn wachtwoord. In de klas is dit misschien ook al een keertje voorgekomen, bijvoorbeed als iemand probeert de inlogcode van de telefoon van een klasgenootje te raden. Bij slecht hacken is er GEEN toestemming gegeven door het persoon dat wordt gehackt.

Als je slecht hackt bestaat er een kans dat je een strafblad krijgt. Een strafblad krijg je als je veroordeelt wordt voor een misdrijf, bijvoorbeeld vandalisme. Een strafblad heeft impact op welke banen je wel/niet kan volgen als je later groot bent. Als je een strafblad hebt, mag je bijvoorbeeld geen hacker meer worden, want je moet ethisch zijn.
[Slide 7]

Goed hacken is als er wel toestemming is. Er zijn mensen die een baan hebben als ethisch/legale hacker. Deze mensen krijgen toestemming van een bedrijf om hun omgeving te hacken. Als ze klaar zijn met hacken krijgt het bedrijf dan te horen waar een slechte hacker binnen kan komen. De goede hacker help het bedrijf vervolgens om zich te beschermen tegen de slechte hackers.

[Slide 8]
Er is zelfs nog een derde manier van hacken, alleen is deze niet zo bekend. Dit is creatief hacken, je gaat hier iets doen met spullen waarvoor ze niet zijn gemakt. De mensen in India zijn hier heel erg goed in! Bijvoorbeeld linksbovenin zie je de wielen van een fiets waar een stoel van is gemaakt.

Bovenin in het midden zie je een scooter die eigenlijk voor 2 personen is, en waar nu 6 personen mee vervoert kunnen worden. Aan de rechterkant zie je ook een leuke hack, waarbij er een plankje mist om je telefoon op te kunnen laden. Dit heeft iemand opgelost met zijn schoen. Het tafeltje links-onderin is gemaakt door Nederlandse hackers, dit is het goedkoopste tafeltje van de IKEA, wat op hacker-conferenties wordt gebruikt in de lounge om hun drankje op te zetten. In het tafeltje zit een router of switch die ervoor zorgt dat je internet hebt.

Het plaatje in het midden onderin laat mooi zien dat niet elke beveiligingsmaatregel nuttig is. De slagboom heeft geen nut, omdat iedereen erlangs kan rijden.

[Slide 9]
De lijn tussen goed en slecht hacken is soms heel erg verwarrend en moeilijk. Rechters en advocaten weten het soms ook niet. Daarom hebben we een regel voor jullie.

[Slide 10]
If you dont own it, you dont pwn it! Dit betekent: als het niet van jou is, dan blijf je er van af.

Klasvraag: Wie heeft er allemaal een game-console, zoals een playstation? Wie denkt dat hij de playstation mag hacken? Waarom? Wie denkt van niet? Waarom niet?

De playstation (of elke andere game-console) mag je eigenlijk niet hacken, doordat deze eigendom is van Sony, met een moeilijk woord noemen we dit ‘Intellectueel Eigendom’. Het hacken van je playstation thuis zit al op die moeilijke lijn of het legaal of illegaal is.

[Slide 11]
Mocht je hacker willen worden, dan is het belangrijk dat je nieuwsgierig bent. Stel heel veel de Waarom? Vraag. Wees benieuwd hoe dingen, systemen werken. Probeer dingen stuk te maken, en ze ook weer beter te maken. Zoek mensen op die je kunnen helpen om je vragen te beantwoorden, of waar je samen mee kan hacken. Het belangrijkste: geef niet op! Blijf doorzetten.

[Slide 12]
Het kan soms zijn dat je per ongeluk iets hebt gehackt. Afhankelijk van welke acties jij zelf onderneemt, kan dit positieve of negatieve gevolgen hebben. Als je niet eerlijk bent over wat je doet en je wordt toch betrapt bestaat er een kans dat je een strafblad krijgt en het dus moeilijker is om een baan te vinden. Om te voorkomen dat dit gebeurd hebben we een aantal regels:

[Slide 13]
Regel 1 is wees eerlijk over wat je hebt gedaan, vertel elk detail en laat geen dingen weg die mogelijk impact kunnen hebben op de situatie. Dit is moeilijk en vervelend, maar het is nog vervelender als bestanden op de gehackte server vertellen dat je toch iets meer hebt gedaan dan jij ooit hebt verteld.

Regel 2 is dat je dit moet vertellen aan een volwassene, dit kunnen je ouders zijn, een docent op school, je oom of tante, of neem contact op met Hack in the Class. Een volwassene kan je helpen om samen op zoek te gaan naar een oplossing.

[Slide 14]
Andere hackers kan je vinden op hackerspaces, dit is een soort van techniekclub waar mensen coole dingen bouwen met bijv. 3D-printers, laser snijders, houtbewerking electronica of heel veel andere mogelijkheden. De Jonge Onderzoekers is ook zo'n techniekclub maar dan voor kinderen onder de 18. In sommige steden bestaat ook CoderDojo, dit is een plek waar kinderen kunnen leren programmeren onder begeleiding van vrijwilligers. Soms heb je ook een gekke docent op school die misschien ook wel een hacker is. Hackers zitten natuurlijk ook online, maar dan weet je niet helemaal wie het is, dus kijk daar wel mee uit. Sommige mensen liegen op het internet wie ze echt zijn.

[Slide 16]
Klasvraag: Wie heeft er weleens zo'n emailtje ontvangen? Wat heb je toen gedaan?

Phishing e-mailtjes zijn nep-emailtjes die informatie of vaak geld van jou willen hebben. Daarom is het belangrijk om bij elk mailtje achterdochtig te zijn of het wel echt is. Als iets te mooi klinkt om waar te zijn, bijvoorbeeld 'Win gratis de nieuwste iPhone!', dan is dit waarschijnlijk ook het geval. Vraag je daarom af: Ken ik het persoon wel? Klinkt dit als waarheid? Sommige mailtjes van klasgenootjes zijn ook phishing-mails, bijvoorbeeld een uitnodiging voor een vreemd of nieuw spelletje. Deze linkjes bevatten soms gevaarlijke code die je telefoon kunnen overnemen.

Als je het niet vertrouwd, gooi het mailtje gelijk weg en klik niet op linkjes in het mailtje.

[Slide 19]
Klasvraag: Heb je je naam weleens ingetypt op een zoekmachine?

- Wat heb je toen gevonden?
- Wist je dat deze informatie op het internet te vinden was?
- Heb je toestemming gegeven dat je informatie gebruikt is?
- Wat vind je ervan?

Als je iets op het internet hebt gevonden over jezelf wat je niet online wilt hebben, dan heb je het recht om dit aan te geven bij de website. Bijvoorbeeld als de voetbalclub een foto online heeft staan van jou, kan je bij de voetbalclub aangeven dat ze de foto moeten verwijderen van de website. Dit kan je ook doen op websites zoals Google, Facebook en Instagram. Deze websites zijn verplicht om je informatie te verwijderen. Mocht je hulp of advies nodig hebben kan je altijd contact opnemen met Hack in the Class.

[Slide 20]
Klasvraag: Wie heeft er weleens de gebruikersvoorwaarden doorgelezen van een website? Kan iemand vertellen wat er in de voorwaarden staat?

De gebruikersvoorwaarden maken vaak gebruik van moeilijk taal die lastig is om te lezen en ze maken de voorwaarden heel erg lang. Dit zorgt ervoor dat de meeste mensen de voorwaarden niet lezen en akkoord gaan zonder te weten waarmee.

Klasvraag: Wie maakt er gebruik van Instagram of Snapchat? Weet iemand wat er met de foto’s en berichtjes gebeurd die op hun platform binnen komen?

[Slide 21]
Alle berichtjes en foto’s die je via Instagram, Snapchat of elke andere grote website verstuurd zijn van dat bedrijf. Dit betekend dat als je een foto plaatst zij de rechten krijgen over de foto. Ze mogen dan alles doen met de foto wat ze willen, bijvoorbeeld gebruiken voor andere doeleinden, verspreiden aan andere personen of bedrijven of in het openbaar gebruiken. Als je bijvoorbeeld een foto hebt waar je heel raar op staat, bijvoorbeeld je bent aan het kwijlen terwijl je aan het slapen bent, of het ziet eruit alsof je in je broek hebt geplast omdat je water hebt gelekt tijdens het handen wassen, dan mogen deze bedrijven deze foto’s gebruiken als poster in bushokjes of op pakken melk in Amerika.
Wees dus bewust van wat je allemaal online zet.

[Slide 22]
Elke dienst waar je gebruik van maakt, bijvoorbeeld Gmail, Maps, Siri, etc. slaat informatie op. Deze informatie is bijvoorbeeld hoe lang je de dienst hebt gebruikt, welke opdracht je hebt gegeven aan de dienst (bijvoorbeeld: hoe loop ik vanaf school naar de dichtsbijzijnde winkel waar ik een joint kan halen). Een hoop van deze informatie bevat gevoelige informatie, bijvoorbeeld als je per ongeluk zwanger bent geraakt en naar een abortuskliniek wilt om de zwangerschap te stoppen, of dat je naar een homo-bar bent geweest. Voor een hoop mensen kan het impact hebben op hun prive-situatie, op werk of binnen geloofsovertuigingen als deze informatie bekend wordt. Wees bewust van elk

stukje informatie wat je opzoekt op het internet, impact kan hebben op je prive-situatie.

[Slide 23]
Klasvraag: Wie van jullie installeert nooit updates op zijn telefoon, tablet of computer thuis? Waarom doe je dit? Wat zijn consequenties van het niet installeren van updates?

Updates installeren is belangrijk, omdat er heel vaak beveiligingsproblemen verholpen worden, die door kwaadaardige of criminele hackers misbruikt kan worden. Door het intsalleren van updates zorg je ervoor dat criminele hackers het moeilijker hebben om jou te hacken.

[Slide 25]
Klasvraag: Wat is een goed wachtwoord?

[Slide 26]
Een goed wachtwoord is lang, hoe langer hoe beter, maar minimaal 10 tekens. Als het kan, probeer dan een wachtwoordzin te maken, bijvoorbeeld: “Op maandag moet ik boterhammen smeren”. Of combineer meerdere regels uit je favoriete liedjes of boek. Probeer voor elke website een ander wachtwoord te gebruiken. Dit is natuurlijk lastig om te onthouden, daarom kan je gebruik maken van een wachtwoordkluis. Dit is een applicatie die je kan installeren op je telefoon of computer die alle wachtwoorden onthoudt en beschermd met een lang hoofdwachtwoord.

[Slide 27]
Het is heel erg lastig om te weten of je wachtwoord weleens gestolen is geweest of niet, gelukkig is er een website waarop je dit kan checken. Als je wachtwoord ooit is gelekt is het handig om je wachtwoord direct aan te passen, ook op alle websites waar je dit wachtwoord ook gebruikt.

We gaan nu op de computer naar haveibeenpwned.com. Vul op die website je e-mailadres in om te kijken of je wachtwoord is gelekt.

[Slide 28]
Nu is het tijd om te hacken!

[Slide 29]
Open je laptop en ga met Firefox en Chrome naar: https://lab.hackintheclass.nl. Je kruipt nu in de huid van een hacker en je moet de administrator van de website hacken.