Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 12
JURIDISCHE- EN ETHISCHE KANT VAN INTERNET

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Informatie over de “Gebruiksvoorwaarden”

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Inhoudsopgave

Auteurs

Francisco de Quinto, Piqué Abogados Asociados

Jordi Saldaña, Piqué Abogados Asociados

Jaume Abella, Enginyeria La Salle (URL) – ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

Translation by Raoul Teeuwen

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

12.1. Inleiding

Nieuwe technologie die veel aspecten van de maatschappij raakt trekt ook minder goed bedoelenden aan: criminelen, zowel individuelen als in groepsverband.
Daarom hebben we deze laatste les gereserveerd om te kijken naar wat juridische- en etische aspecten, waarbij we kijken naar gedrag dat kan leiden tot wets-overtredingen en de gevolgen daarvan.

12.2. Buitenlandse criminaliteit en binnenlandse rechten

Zoals hiervoor gesteld: introductie van nieuwe technologie trekt vaak ook boeven aan. Er zijn grofweg twee manieren Informatie Technologie en Communicie-technologie (ITC) kan leiden tot criminaliteit:
1. Technologie kan nieuwe manieren bieden om op een traditionele ('oude') manier de wet te overtreden. Het gaat daarbij om illegale activiteiten die ook zijn genoemd in het wetboek van strafrecht, maar die nu op een nieuwe manier worden uitgevoerd. Voorbeelden zijn het witwassen van geld en illegale vormen van pornografie.
2. Daarnaast vinden boeven vaak een heel nieuwe vorm van criminaliteit uit met nieuwe technologie, en vaak moeten wetteksten worden aangepast/aangevuld om te zorgen dat ook die nieuwe criminele activiteiten kunnen worden aangepakt. Voorbeelden zijn verspreiding van spam en virus-aanvallen.

Een ander kenmerk van ITC is het gebied waarop ze betrekking hebben: niet alleen de directe omgeving, maar vaak zijn ook andere landen betrokken.
Vóór het verschijnen van ITC was van wetten vaak duidelijk wie er rechtspraken mocht doen en welke wetten daarbij van toepassing waren. Die beide concepten zie je nog steeds bestaan en zijn nog steeds gebiedsgebonden.
Samenvattend kun je stellen dat ITC wereldomspannend is en meerdere landen raakt, terwijl de wet en de rechtbanken nog bijna geheel gebaseerd zijn op landen en landsdelen. En de verwarring is nog groter dan hij in eerste instantie lijkt. Want alhoewel je er niet bij stil staat, kan het verkeer tussen een gebruiker in Barcelona en een website die gehost wordt bij een ISP in Californie wel langs 10 ISPs gaan, die allemaal in andere delen van de wereld zitten.
In dit soort situaties is het belangrijk om te bepalen welke wetten van welk land van toepassing zijn bij overtredingen. Welke rechtbank in welk land moet betrokken worden?
In november 2001 ondertekende 30 landen, waaronder 15 partners van de Europese Unie, de Verenigde Staten, Canada, Japan en Zuid Afrika, in Budapest een overeenkomst van de Europese Commissie rond cyber-crime. Die overeenkomst moet een deel van de 'nieuwe problemen' als gevolg van ITC aanpakken en is het resultaat van 4 jaar werk en omvat een document met 48 artikelen die zijn verdeeld over vier categorien:
1. Inbreuk op de vertrouwelijkheid
2. Vervalsing en coomputer fraude
3. Inbreuk met betrekking tot content
4. Overtredingen van de auteursrechten

5

Nadat de, bijzonder complexe, regelgeving en straffen (sancties) op gebied van internet criminaliteit zijn beschreven, moeten er nog overeenstemming worden bereikt op drie gebieden:

1ste uitdaging: wie mag recht spreken. Hoe kies je de instantie/rechtbank die een grensoverschrijdende zaak gaat afhandelen. Dit probleem wordt nog niet eenduidig opgelost door huidige juridische systemen.
2de uitdaging: wetsconflicten. Zodra bekend is wie rechts gaat spreken, moet worden bepaald welke wetten dan gebruikt worden. Ook hier blijkt dat traditionele systemen niet zijn voorbereid op de nieuwe virtuele wereld.
3de uitdaging: uitvoeren van de uitspraak. Zodra een rechtbank een uitspraak heeft gedaan, moet die uitspraak ook worden uitgevoerd, mogelijk door een andel land dan dat de uitspraak heeft gedaan. Dan is het wel nodig internationaal af te spreken dat de uitvoerder zich houdt aan de uitspraak, anders komt er van dit hele systeem steeds minder terecht. Dit lastige punt is nog lastiger op te lossen dan de eerdere twee punten.
Een voorbeeld van hoe lastig dit is blijkt uit de zaak van een Russische cracker die Amerikaanse systemen had gehacked en daarop voor een interview was uitgenodigd door een Amerikaans nep-bedrijf.
Tijdens het interview demonstreerde hij zijn vaardigheden door zijn eigen netwerk in Rusland te hacken. Toen wisten de interviewers, die FBI-agenten waren, genoeg en arresteerden hem. De FBI gebruikte sniffers op de interview-computer om vervolgens al het bewijs te verzamelen, ook op de computer in Rusland., om zo een veroordeling zeker te stellen.
Maar er waren de nodige vraagtekens bij deze zaak:
● Mocht de FBI wel bewijs verzamelen op een computer in Rusland, zonder toestemming van de Russische autoriteiten?
● Door hem uit te nodigen voor een gesprek in de VS hoefde de FBI geen uitleveringsbewijs te regelen om de hacker achter slot en grendel te plaatsen, maar was dat wel legaal?
● Kon de Verenigde staten een persoon wel veroordelen voor criminele zaken die technisch gezien op Russisch grondgebied werden gepleegd?
Uiteindelijk werd hij in de VS veroordeeld, omdat hij bij een deel van zijn aanvallen een in de VS opgestelde proxy server had gebruikt. Hij kreeg 4 jaar gevangenisstraf en woont en werkt nu in de VS.
Oefening:
Bespreek minimaal 1 van de vragen (onderzoek van een computer die in een ander land staat; uitnodiging of uitlokking (?) om uitleveringsprocedures te ontlopen; veroordeling voor internet-criminaliteit tegen een buitenland), waarbij zowel de kant van white hats (de goed bedoelende hackers) als de kant van de black hat (de kwaad bedoelende hackers) wordt bekeken.

1. Bespreek eerst in je groep waarom het waarschijnlijk legaal was, en schrijf de redenen daarvoor op.
2. Kies nu de andere kant, en bespreek waarom het illegaal was en schrijf op waarom dat zo is.
3. Als je dit in een klas of groep uitvoert, kijk dan of je na het werken in kleine groepjes, nu met de hele groep overeenstemming kunt bereiken.
Bedenk dat het hier vooral gaat om de discussie: er is niet persé een goed antwoord, en in de meeste landen wordt nog gewerkt om dit soort criminaliteit helder aan te pakken en op te lossen.

12.3. Aan ITC gerelateerde misdaden

Het in een categorie indelen van crimineel gedrag is één van de basisprincipes van veel juridische systemen. Je kunt potentiele criminele acties indelen in 6 groepen.
1. Manipuleren van gegevens in bestanden of op andere computer systemen.
2. Zonder toestemming toegang tot gegevens verkrijgen of gegevens gebruiken.

3. Programma's of routines in een andere computer inbrengen om gegevens of programma's aan te passen of te verwijderen.
4. Gebruik van de computers of programma's van een ander zonder zijn/haar toestemming, met als doel eigen gewin of schade toebrengen aan anderen.
5. Gebruik van de computer met frauduleuze bedoelingen.
6. Aanval op de privacy door gebruik van persoonsgegevens op een andere manier dan waarvoor toestemming is gegeven.

Technische criminaliteit wordt gekenmerkt doordat het lastiger te ontdekken, bewijzen en aan te klagen is. Slachtoffers kiezen er vaak voor om de gevolgen te dragen, een poging te doen herhaling te voorkomen in plaats van een juridische procedure op te starten. Daardoor wordt het lastig om te bepalen hoe veel criminele activiteit er voorkomt en om er wettelijke maatregelen tegen te nemen.
De situatie wordt nog eens verergerd door de snelheid waarmee de technologie verandert. Dat weerhoudt wetgevers er echter niet van om zich aan te passen en waardevolle hulpmiddelen te maken waarmee rechters, advocaten en andere betrokkenen dit soort ITC-criminaliteit kunnen bestraffen.
Hierna willen we een aantal specifieke criminele activiteiten behandelen die gerelateerd zijn aan ITC.
1. Jezelf als een ander voordoen: de anonimiteit van het internet stelt mensen in staat zich anders voor te doen dan wie ze zijn. Dit kan leiden tot criminaliteit, als mensen dit gebruiken om informatie te verzamelen of om het vertrouwen van anderen te winnen.
2. Onderscheppen van communicatie: onderscheppen van geheimen of prive informatie in emails of telefoongesprekken.
3. Ontdekken en publiceren van geheimen: bedrijfsgeheimen ontdekken door illegaal informatie te bekijken. In sommige gevallen worden uitspraken omvangrijker als de geheimen worden doorgegeven aan een andere partij.
4. Ongeautoriseerde toegang tot computers: illegale toegang tot accounts en informatie, met als doel het behalen van winst. Dit omvat ook identiteits-diefstal.
5. Schade toebrengen aan computerbestanden: vernietigen, aanpassen of op enige manier onbruikbaar maken, van gegevens, programma's of documenten op andere computers, netwerken en systemen.

7

6. Illegaal kopieeren: illegaal kopieeren van auteursrechterlijk bescherm materiaal zonder toestemming van de rechthebbende.

Oefening:
1. Kies één van de bovenstaande onderwerpen en voer de volgende zoektochten uit:
● Zoek een juridische zaak die valt in de gekozen categorie.
● Is er een uitspraak gedaan, en zo ja, is de straf ook uitgevoerd?
● Waarom hebben de daders de misdaad begaan?
2. Met betrekking tot auteursrechten: zijn de volgende acties een misdaad?
● Een (foto)kopie maken van een geheel boek
● Een muziek CD kopieeren die we niet hebben gekocht
● Een muziek CD kopieeren die je wel hebt gekocht
● MP3's, films etc downloaden vanaf/via het internet
● Hoe zou je het vinden als jij artiest was van die muziek of film en geen geld kreeg omdat het alleen maar illegaal werd gedownload of zelfs door anderen werd verkocht als hun eigen materiaal?

12.4. Voorkomen van misdaad en dubbel te gebruiken technologie

De enige betrouwbare manier om voorbereid te zijn op criminele agressie op gebied van ITC is om beveiligings-acties te ondernemen op gebieden die de voorgaande HHS-hoofdstukken zijn behandeld. Daarbij is het van belang die maatregelen zo te nemen dat het bijna onmogelijk wordt om crimineel- of twijfelachtig gedrag te vertonen.
Het is belangrijk te beseffen dat technologie dubbel kan worden gebruikt: niet alleen om te beveiligen, maar ook voor criminele activiteiten. Denk bijvoorbeeld aan cryptografie en technologie die gebruikt wordt om electronische communicatie te onderscheppen. In deze paragraaf gaan we daar dieper op in, en op de ernstige gevolgen, ook op gebied van beleid, sociale aspecten, economische aspecten en onderzoek.

12.4.1. Het wereld-omspannende bewakingssysteem: "COMINT"

De kreet COMINT is recent ontstaan door de combinatie van "COMmunications INTelligence" en heeft betrekking op het onderscheppen van communicatie die het gevolg is van ITC. Tegenwoordig kun je een goede boterham verdienen met COMINT, door klanten, zowel overheid als bedrijfsleven, op verzoek te voorzien van slimme gegevens, vooral op gebied van diplomatie, economie en onderzoek. Daardoor is het oude systeem waarbij het vooral militairen waren die geheim alles afluisterden, vervangen door een meer open systeem van nieuwe technologieen om data te verzamelen en bestuderen. De bekendste voorbeelden van COMINT technologie zijn de systemen "ECHELON" en "CARNIVORE", die we hierna behandelen.

12.4.2."ECHELON"

Het systeem is rond 1947 ontstaan, net na de 2de wereld oorlog, in een overeenkomst tussen het Verenigd Koninkrijk en de Verenigde Staten met duidelijke militaire- en beveiligingsdoelstellingen. De details van de overeenkomst zijn nog steeds niet publiek bekend. Later hebben landen als Canada, Australie en Nieuw Zeeland zich aangesloten.
Het systeem werkt door eenvoudigweg enorme hoeveelheden communicatie te onderscheppen, los van de manier van transport of opslag, maar met nadruk op de volgende gebieden:
• Breedband uitzendingen (wideband en Internet)
• Fax en telefoon-communicatie via de kabel: onderscheppen van kabels, en onderzeeers met behulp van speciaal hiervoor uitgerustte schepen
• Communicatie per mobiele telefoon
• Stem herkennings systemen (VRS-en)
• Biometrische Systeem Herkenning, zoals gezichtsherkenning via anoniem filmen
Later wordt uit die berg de waardevolle informatie gefilterd, met behulp van zaken als Kunstmatige Intelligentie (Artificial Intelligence (AI)) om sleutelwoorden te herkennen.
Elk van de 5 leden stelt een sleutelwoorden-lijst ter beschikking waarop gefilterd wordt.
Uiteraard veranderen die lijsten in de loop van de tijd. Nadat het systeem in het begin vooral voor militaire en beveiligings-doeleinden (terrorisme, wapen- en drugshandel, dictators etc) werd gebruikt, maar later kreeg het ook een rol op gebied van wereldwijde economie, commercieel beleid in bedrijven etc.
Recent werkt ECHELON in een vorm van een ster met 5 punten, rond 2 hoofd-punten.

Beide punten staan onder controle van de NSA (National Security Agency): één in de Verenigde Staten, samenvallend met het NSA hoofdkwartier in Fort Meade (Maryland), en de ander in Engeland, noord van Yorkshire, met de naam Meanwith Hill.
Op de punten van de ster staan volgstations van de deelnemers aan ECHELON:

- De Verenigde Staten(2): Sugar Grove en Yakima.
- Nieuw Zeeland (1): Wai Pai.
- Australie (1): Geraldtown.
- Verenigd Koninkrijk(1): Morwenstow (Cornwell).
- Er was er nog één in Hong Kong voordat dat gebied werd terug gegeven aan China.

12.4.3. "CARNIVORE"

Het tweede grote wereldomspannende systeem voor onderschepping en spionage wordt gefinancierd door de FBI (Verenigde Staten) en staat bekend als CARNIVORE, met als publieke doelstelling het bestrijden van georganiseerde misdaad en bijdragen aan de beveiliging van de Verenigde Staten. Door de vooruitstrevende krachtige technologie en zijn veelzijdigheid, krachtige luisterfunctionaliteit en mogelijkheden om te veranderen van aandachtsgebied is het rond CARNIVORE tot een botsing gekomen met de politiek (US Congress) en de massa media.
9

CARNIVORE is ontwikkeld in 2000, is een automatisch systeem, en onderschept internet communicatie. De Amerikaanse privacy-voorvechters-organisatie protesteerde tegen CARNIVORE als de zoveelste aanval op de privacy. Een andere groep, de Electronic Privacy Information Center (EPIC) heeft verzocht dat een federale rechter de FBI dwingt ISP's toegang te geven tot het bewakingssysteem – om zeker te stellen dat het systeem niet voor dingen wordt gebruikt die buiten de wet vallen.
In Augustus 2000 wees een rechter een wetsvoorstel af waarmee de FBI de mogelijkheid had gekregen om (vooral mobiele communicatie) af te luisteren zonder voorafgaande toestemming van een rechter.
Deze twee voorbeelden laten zien dat de FBI de bedoeling heeft van CARNIVORE een systeem te maken om alle communicatie binnen de Verenigde Staten af te luisteren. Het project is in meerdere staten verboden omdat het de burgerrechten van Amerikanen aantast, in ieder geval in die 1ste versie. Formeel is gesteld dat er kritisch naar het project wordt gekeken.
Oefening:
Een aan deze COMINT-systemen gerelateerde grap is te vinden op internet. We nemen hem hier op voor discussie in de klas/groep over de ethische en juridische gevolgen:

Een oude Irakese Moslim die al 40 jaar in Chicago woont, wil al tijden aardappelen verbouwen in zijn tuin, maar hij is niet in staat de grond daarvoor om te ploegen. Zijn enige zoon, Amhed, studeert in Frankrijk. De oude man stuurt zijn zoon een email waarin hij het probleem uitlegt:

"Amhed, ik vind het jammer dat ik dit jaar geen aardappels zal hebben in mijn tuin. Ik ben te oud om de grond om te ploegen. Als jij hier zou zijn, zouden mijn problemen verdwijnen. Ik weet dat jij die grond dan wel voor me zou omploegen. Liefs, je vader. "

Een paar dagen later ontvangt de man via email een reactie van zijn zoon:
"Vader: in Gods naam, blijf van de tuinaarde af. Daar heb ik mijn .... verborgen. Liefs, Amhed.
"

De volgende morgen om 4:00 staan de lokale politie, FBI, CIA, S.W.A.T teams, de RANGERS, de MARINES, Steven Seagal, Sylvester Stallone en nog wat meer sterke mannen op de stoep en beginnen gelijk alle grond af te graven en onderzoeken op zoek naar onderdelen waarmee pompen, anthrax of ander spul te maken is. Ze vinden niets en druipen weer af.

Dezelfde dag ontvangt de man weer een email van zijn zoon:
"Vader: ik neem aan dat de grond nu geschikt is om aardappelen in te poten. Het was de beste manier die ik onder deze omstandigheden kon bedenken. Liefs, Ahmed."
10

Oefening:
Zoek op internet naar informatie over Echelon en Carnivore en kijk of je ook informatie kan vinden over hun toepassing op netwerken en ITC-systemen in je eigen land en beantwoord de volgende vragen:
1. Waar staat de kreet "ECHELON" voor?
2. Uit welke onderdelen bestaat ECHELON?
3. Uit welke onderdelen bestaat CARNIVORE?
4. Zoek naar een spraakmakend voorbeeld waarbij ECHELON en een bekende persoon worden genoemd.
5. Zoek naar een voorbeeld van toepassing van CARNIVORE gerelateerd aan een wereldbekende terrorist.
6. Wat is jouw mening over de toelaatbaarheid van zulke systemen?

12.5. Ethical Hacking

Behalve dat we praten over crimineel gedrag, misdaden en de gevolgen, moeten we ook duidelijk maken dat niet elke hacker een crimineel is.
Tegenwoordig huren bedrijven zelfs “Ethische Hackers" in om kwetsbaarheden in hun systemen te vinden om daarmee hun beveiliging verder te verbeteren.
Ethische Hackers helpen met hun kennis continu te bewaken dat alles goed bewaakt is. Ze voeren
"gecontroleerde" aanvallen uit, vooraf afgesproken met de betreffende organisatie, om de systeembeveiliging te testen.
Ze vormen groepen om informatie uit te wisselen over nieuwe aanvallen, nieuwe kwetsbaarheden etc. Ze zijn onderzoekers op gebied van beveiliging.
Sun Tzu zei in zijn boek "The Art of War", "De aanval is het geheim van de verdediging; verdediging is het plannen van een aanval".
Het ethisch hacken kent een aantal fases:
1. Aanvalsplanning
2. Internettoegang
3. De aanval testen en uitvoeren
4. Informatie verzamelen
5. Analyse
6. Assessment en Diagnose
7. Afsluitend Rapport
Een bruikbaar hulpmiddel dat Ethisch Hackers gebruiken is de OSSTMM methode - Open Source Security Testing Methodology Manual. Deze methode kan worden gebruikt voor het testen van elk beveiligingssysteem, van een bewaker en een deur tot mobiele- en satteliet-communicatie. De methode is toegepast door organisaties als Spaanse Financiele instituten, de Amerikaanse Luchtmacht en Marine, het Amerikaanse Ministerie van Financien (om financiele instellingen te testen)

Oefening:

- Zoek informatie over Ethisch Hacken en de rol ervan binnen IT beveiligings bedrijven.
- Zoek informatie over het OSSTMM en soortgelijke methodes.

Zoek informatie over certificering van Ethische Hackers.

12.6. De 10 meest voorkomende internet fraudes

Hieronder vind je een samenvatting van de Federal Trade Commission van de meest voorkomende misdaden op internet (2005).
1. Internet veilingen: Nadat klanten hun geld hebben overgemaakt krijgen ze een pakje van een lagere waarde of, nog erger, geheel niets.
2. Internet Toegangs Diensten: Consumenten worden verleid tot het aangaan van meerjarige contracten voor internetdiensten, terwijl ze er alleen tegen hoge kosten eerder vanaf kunnen.
3. Credit Card Fraude: fraudeurs vragen op een site je credit card nummer waarna je gratis toegang wordt beloofd tot allerlei moois, maar achteraf blijkt je credit card toch misbruikt te worden voor aankopen.
4. Internationaal inbellen: er wordt stiekum of 'gratis' een 'handig' programma geinstalleerd, maar dat blijkt dure buitenlandse nummers te bellen en jaagt je zo op kosten.
5. Web Cramming: er wordt je iets voor een gratis proefperiode aangeboden, maar na die perode blijkt dat je toch de rekening krijgt voor van alles, zonder dat je daarmee hebt ingestemd.
6. Multilevel Marketing Plannen/ Pyramides: er wordt je beloofd dat je rijk wordt omdat van alles wat je zelf EN door jou aangebrachte nieuwe verkopers, wordt verkocht, een aandeel ontvangt. Achteraf blijkt dat je je in moet kopen bv voor een starterspakket, maar dat het vinden van andere verkopers vies tegenvalt en het je dus vooral geld kost.
7. Reizen en Vakantie: je tekent op voor dat mooie aanbod van een luxe reis voor een prikkie, maar dat blijkt in de praktijk stukken minder mooi dan op de plaatjes of je krijgt geheel niets.
8. Zakenkansen: er wordt je een mooi verhaal voor gehouden waarmee ook jij eenvoudig een zaak kunt beginnen en rijk kunt worden, maar die zakenkans maakt je vooral armer en de inkomsten blijken toch niet zo makkelijk te behalen zijn.
9. Investeringen: koop je flink in in kansrijke bedrijven ... achteraf blijkt dat die bedrijven toch niet zo kansrijk waren en de waarde van aandelen, opties etc valt tegen.

12

10. Gezondheidsprodukten/-Diensten: een produkt wordt geadverteerd als de oplossing voor een ziekte of probleem, mensen die aan de aandoening lijden kopen het, maar de werking blijkt tegen te vallen.

Oefening:
Denk even na over de volgende vragen en bespreek ze in je groep:
1. Denk je dat jij ook in de trucen zou kunnen trappen van de oplichters die we hiervoor hebben behandeld?
2. Een quote van een ISECOM directielid: “Om de juiste achtergrond te hebben om de beveiligingstoestand van een computersysteem te kunnen beoordelen, of zelfs van een hele organisatie, moet iemand grondig begrip hebben van beveiligingsmechanismes, en kunnen meten hoeveel vertrouwen je mag stellen in die beveiligingsmechanismes”.
Bespreek in je groep wat met die uitspraak bedoeld wordt en hoe je je kunt voorbereiden om “de beveiligingstoestand van een computersysteem te kunnen beoordelen”. Heb je na deze lessenserie genoeg materiaal om een goed begin te hebben/maken?
3. [oefening die je eventueel kunt maken, maar dan niet in een groep, maar individueel]: na deze les kan het gebeuren dat er dingen zijn waarover je hebt gehoord of die je wellicht zelfs

hebt uitgeprobeerd, waarvan je dacht dat dat mocht, maar waarvan je je nu afvraagt of het allemaal wel legaal was. Zoek dan eens op internet meer informatie: meestal vind je dan het antwoord wel.

12.7. Verder lezen

http://www.consuwijzer.nl/?WT.srch=1
http://www.eccnl.eu/page/nl/over-ecc/Over-ECC
http://klachten.internetadressenwijzer.nl/
http://www.internetoplichting.nl/
http://digibewust.nl/
zoek op google op "internet scams site:.nl"
http://nl.wikipedia.org/wiki/Carnivore_(software)
http://nl.wikipedia.org/wiki/ECHELON
http://www.isecom.org/