Mediawijsheid 2: Veiligheid

Inleiding

Internet is niet meer alleen een plek waar je informatie kan vinden (web 1.0). Iedereen kan er tegenwoordig informatie plaatsen: via fora, weblogs, sociale netwerken etc. Maar je kunt er ook online aankopen doen, je bankzaken regelen een weblog bijhouden, foto's plaatsen etc. We spreken nu van Web 2.0.

Cursisten zijn tegenwoordig de hele dag online. Hoe kun je hen wapenen tegen de gevaren van dit internetgebruik?

Bekijk eerst eens het filmpje What the H@ck, gemaakt door cursisten van ROC Midden Nederland waarin de onveilige manier van werken door docenten op de hak wordt genomen:

Maar ook voor andere collega's van het Nova College kan dit een leerzaam arrangement zijn. Voor iedereen is veilig online werken tenslotte belangrijk. Bekijk de film over de Familie van der Ploeg

Onze cursisten zijn in de leeftijdsgroep vanaf 16 jaar. Dit arrangement is dan ook geschreven voor docenten die lesgeven aan deze doelgroep.

SBU: 8

Dit arrangement maakt deel uit van de digitale leerlijn "De docent competent!" van het Nova College. Klik hier voor het hoofdarrangement.

Auteur: Bernadet Sprenkeling, ROC Nova College

Persoonlijke informatie

Wees heel voorzichtig met persoonlijke informatie. Plaats je naam, adres, geboortedatum, e-

mail en telefoonnummer niet op het internet. Je kunt het beste gebruik maken van een Nick-name of schuilnaam. Des te meer gegevens er van je online te vinden zijn, des te groter de kans dat er misbruik van gemaakt kan worden.
Identiteitsfraude

Oefening:
Voer een "ego-surf"of "ego-search" uit, dwz. zoek op je eigen naam of adres met Google of met een andere zoekmachine zoals http://wieowie.nl/. Kijk wat er allemaal bekend is over jou op internet. Schrik je ervan?

Wachtwoorden

Wat is een veilig wachtwoord?

Verzin een wachtwoord dat niet voor de hand ligt. Dus bijvoorbeeld niet je geboortedatum of de naam van je huisdier.
Een veilig wachtwoord bestaat uit tenminste hoofdletters, kleine letters, en tenminste een cijfer of speciaal teken. Verander je wachtwoord ook regelmatig.

Geef je wachtwoorden nooit door aan anderen, ook al is het nog zo'n goede vriend!

Meer informatie over zwakke en sterke wachtwoorden

TIP: Gebruik de eerste letters van de woorden in een zin die je makkelijk kan onthouden (bijvoorbeeld "Meneer van Dale wacht op antwoord" wordt mvdwoa) en zet daarachter een vreemd teken met getal dat je steeds aanpast als je je wachtwoord moet wijzigen. Zo kan een goed wachtwoord zijn: mvdwoa?1

Chatten

Chatten kan erg leuk zijn om te doen. Chat alleen met bekenden dus bijvoorbeeld via Hyves, Skype, Facebook of MSN. Dit is de veiligste manier van chatten. Op deze sites kun je de chatsessie ook opslaan. Mocht er dan iets vervelends gebeuren (je wordt bijvoorbeeld gepest via MSN), dan kun je de chatsessie uitprinten en bespreken met anderen wat je er het beste aan kunt doen.

Wil je toch chatten via een chatsite, gamesite of forum, let dan op de volgende punten:

- Gebruik een schuilnaam, nooit je eigen naam
- Geef geen persoonlijke informatie of foto's aan degene met wie je chat
- Zet nooit je webcam aan

- Beantwoord geen vragen die je niet wilt beantwoorden
- Stop direct met chatten als het niet goed voelt
- Maak nooit een echte afspraak met iemand met wie je chat

E-mailen

Phishing e-mails, spam en kettingmail

Ook e-mailen kan gevaren met zich meebrengen.
Zorg altijd voor een goede virusscanner, bijvoorbeeld het gratis programma AVG. Virussen worden vaak meegezonden met e-mails als bijlage. Open dan ook geen bijlagen en/of e-mails van onbekenden of onduidelijke afzenders.

Een **phishing e-mail** is een e-mail waarmee men probeert persoonlijke gegevens als pincode of creditcard te achterhalen. Vaak lijkt het of deze e-mail van een bank afkomstig is.Geef nooit via de e-mail persoonlijke gegevens als wachtwoorden, pincodes en creditcardnummers door!

Spam

Een goed SPAMfilter is tegenwoordig onontbeerlijk. Je kunt het krijgen van Spam ook zoveel mogelijk voorkomen door geen dubieuze mails te openen of te beantwoorden. Spam komt ook vaak binnen nadat je je e-maildres hebt doorgegeven voor online spelletjes of prijsvragen etc. Je kunt voor dit soort zaken daarom beter een tijdelijk e-mailadres bij Google of Hotmail aanmaken.

Kettingmail

Kettingmails zijn nog steeds populair onder jongeren. Vaak zijn deze mails alleen maar bedoeld om e-mailadressen te verzamelen voor spam. Niet aan mee doen dus. Hoe zielig het verhaal ook is.

Wat stuur ik door?

Kijk bij het doorsturen van e-mails altijd even in de berichtgeschiedenis. Staat er iets in wat niet voor de nieuwe ge-adresseerde bedoeld is? Soms wordt vertrouwlijke informatie ongewild doorgestuurd. Dit is te voorkomen door even naar beneden te scrollen en de hele inhoud van de berichtgeschiedenis te lezen en desgewenst te verwijderen.

Sociale netwerken

Iedereen is tegenwoordig wel lid van een of ander sociaal netwerk. Denk aan Hyves, Facebook, Linked-in, etc.

Deze netwerken zijn min of meer afgeschermd. Bij de instellingen kun je aangeven wie wat mag zien van jouw profiel. Je kunt meestal kiezen uit:

1. Alleen mensen in je netwerk, dus je vrienden, kunnen alles zien
2. Niet alleen je vrienden maar ook de vrienden van je vrienden
3. Iedereen, in dit geval zet je alles dus eigenlijk open voor de hele wereld.

Daarbij kun je vaak ook nog onderscheid maken tussen wat je voor wie openzet, bijv. telefoonnummer, geboortedatum en adres alleen voor vrienden.

Ook al heb je alles afgeschermd en ingesteld op alleen zichtbaar voor vrienden, realiseren wij ons meestal niet, dat deze vrienden wel van alles van ons kunnen kopieren. Stel je hebt allerlei foto's op hyves geplaatst, maar wil ze er later weer afhalen. Dan kunnen anderen deze foto's al gekopieerd hebben en op hun "Hyves" geplaatst hebben. Zeker onder jongeren waar de vriendenkring regelmatig wisselt kan dit soms nare gevolgen hebben. Plaats dus alleen foto's en filmpjes op internet waar je later geen spijt van krijgt. Want iets erop zetten is makkelijk, eraf halen is lastiger en soms zelfs onmogelijk.

Kan ik als docent cursisten toevoegen op mijn Hyves of Facebook?
Het kan wel, maar is het slim? Sociale netwerken als Hyves en Facebook worden voornamelijk gebruikt voor de familie en vriendenkring. Wil je wel dat cursisten toegang krijgen tot jouw privé leven? Want dat is wat je doet als je ze toegang geeft. Een vriendschapsverzoek van een cursist via Hyves of Facebook kun je dus beter negeren.
Wil je toch via Facebook of Hyves communiceren met cursisten, maak dan een apart profiel aan, een die niet gelinkt is aan je privé-profiel. Maar ook dan moet je jezelf de vraag stellen of je geconfronteerd wilt worden met het privéleven van de cursist.

Solliciteren? Check eerst je Hyves

Meer informatie over de gevaren van Sociale netwerken

Twitter

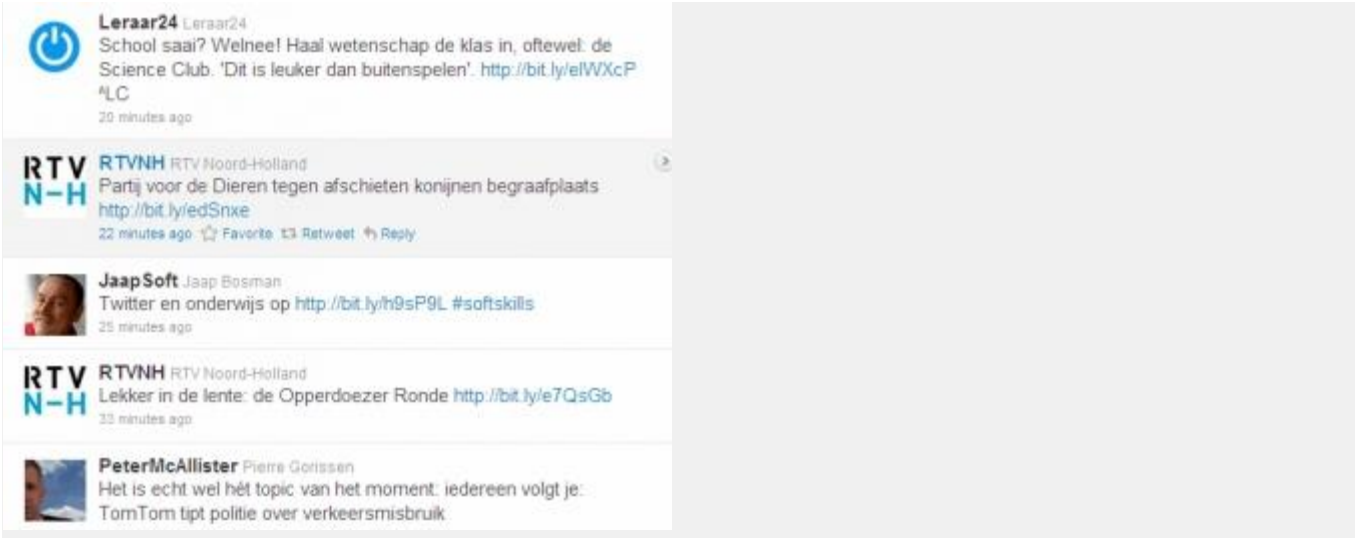
Twitter wordt steeds populairder in Nederland. Met Twitter kun je snel korte berichtjes de wereld insturen. Dit wordt ook wel micro-bloggen genoemd. Wat niet iedereen zich realiseert, is dat Twitter standaard openbaar is. Iedereen kan je berichtjes lezen, dus ook je baas en ook je ex-vrienden of kwaadwillenden. Wil je dit voorkomen, dan zul je in de instellingen eerst moeten aangeven dat je een gesloten account wilt.

Het is niet zo handig om te twitteren dat je een weekendje weg gaat. Wel handig voor die

inbreker.
Op Twitter heb je volgers, maar ook mensen die je niet volgen kunnen jouw berichtjes lezen. Zo gebeurt het steeds vaker dat mensen op hun werk in de problemen komen omdat ze bepaalde dingen getwittert hebben waar de baas niet zo blij mee is. Een politieagente kreeg bijvoorbeeld een melding binnen en twitterde dat het wel om huiselijk geweld zou gaan. Ze werd geschorst. Ook "tweets" die schadelijk zijn voor het bedrijf waar je werkt, kun je maar beter niet versturen. Het kan je zomaar je baan kosten. Tweederde van de werkgevers googled sollicitanten eerst op het internet en hierdoor gaan heel veel brieven direct de prullenbak in.

Jongeren gebruiken Twitter als MSN of Whatsupp, ze vergeten daarbij dat Twitter standaard openbaar is. Tweets vanuit de kroeg met een leuke foto erbij blijken achteraf niet altijd leuk te zijn. Je kan de tweet dan wel weer verwijderen, maar als hij al geretweet is, heb je er geen controle meer over.

Dus bedenk voor je iets twittert:
- Vind ik dit morgen ook nog leuk?
- Beledig ik niet iemand met deze tweet?
- Mag mijn baas dit lezen?
- Wil ik dat de hele wereld dit berichtje kan lezen?



Beveilig je computer

Virussen, spyware, keylockers allemaal zaken die onze computers met zijn data bedreigen. Het is belangrijk om een goed antivirus, anti-spam en anti-spyware programma te installeren en deze natuurlijk ook uptodate te houden. Stel het programma zo in dat hij regelmatig je hele computer scant op malware.
Op de site van Computer-Idee staan: De 10 grootste bedreigingen voor onze pc

Eindopdracht

A. Opdracht voor buiten de les

1. Welke regels zijn er op school met betrekking tot internet gebruik en veiligheid? Verzamel deze.

2. Zoek naar informatie over je cursisten op het internet. Beschrijf hoe "mediawijs" je cursisten naar jou mening zijn. Hebben ze veel privacy gevoelige informatie op het internet staan? Bespreek je bevindingen met je cursisten.

B. Opdracht voor in de les

Laat je cursisten zelf op zoek gaan naar informatie over zichzelf en/of elkaar. Laat ze ernaar kijken met de ogen van bijv. de nieuwe baas waar ze gaan solliciteren.

Plaats een verslag van bovenstaande opdrachten in je portfolio.

Bronnen

Mediawijzer van Kennisnet: http://www.schoolpost.nl/pdf/kennisnet/kn081-mediawijzer.pdf

Waarschuwingsdienst van Ministerie van binnenlandse zaken: Waarschuwingsdienst
Prodocent: Veiligheid en privacy op het web

Mediawijzer expertisecentrum

Wifiwijs.nl: Alles over veilig mobiel (internet) gebruik