



Ideen und Lektionsvorschlag

«Teil 10: Phishing»

Informationen zur Unterrichtseinheit	Seite 2
Grundlagen für die Lehrperson	Seite 3
Vorbereitung	Seite 4
Einstieg mit den Schülerinnen und Schülern	Seite 5
Ablauf der Unterrichtseinheit	Seite 6
Auswertung der Resultate	Seite 7
Anhang, Links	Seite 8



Kampagne für Persönlichkeitsschutz

Seite 2

Informationen zur Unterrichtseinheit

Die vorliegende Unterrichtseinheit beschäftigt sich mit dem Thema «Phishing». Dabei werden die Schülerinnen und Schüler auf das Thema sensibilisiert und erarbeiten präventive Verhaltensmassnahmen für ihre Freizeit und in der Schule.

Mit dem «Medienkompass 2» des Zürcher Lehrmittelverlages steht ein adäquates Lehrmittel zur Verfügung, welches in jede Lehrerbibliothek gehört.

Zielgruppen

Lehrpersonen, Schülerinnen und Schüler der Mittel- und Oberstufe im Alter von 10 bis 14 Jahren.

Arbeitsformen und Zeitfenster

Die Schülerinnen und Schüler arbeiten im Klassenverband, in kleinen Gruppen und auch in Einzel- oder Partnerarbeit am Computer. Eine Internet-Verbindung ist vorteilhaft.

Lernziele

Schülerinnen und Schüler erhalten eine Übersicht ins Thema «Sicherheit – äussere Gefahren im Internet».

Schülerinnen und Schüler kennen Formen von «Phishing».

Schülerinnen und Schüler sind sich bewusst, dass ihr Verhalten wesentlich zu einem sicheren Surfen im Internet beiträgt.



Grundlagen für die Lehrperson

Zu «Phishing» liefert Wikipedia folgende Erklärung: Phishing werden Versuche von Tätern genannt, an Daten eines Internet-Benutzers zu gelangen, z. B. über gefälschte www-Adressen, E-Mail oder Kurznachrichten, um die Benutzer zu schädigen (Kontoplünderung). Der Begriff ist ein englisches Kunstwort, das sich an «password fishing» (bildlich das «Angeln nach Passwörtern mit Ködern») anlehnt. <http://de.wikipedia.org/wiki/Phishing>
Weitere Informationen bieten die zahlreichen Links im Anhang dieser Lerneinheit.

Zu «Hoax» liefert Wikipedia folgende Erklärung: Als Hoax (engl. für Jux, Scherz, Schabernack; auch Schwindel) wird heute meist eine Falschmeldung bezeichnet, die in Büchern, Zeitschriften oder Zeitungen, per E-Mail, Instant Messenger oder auf anderen Wegen (z. B. SMS, MMS oder soziale Netzwerke) verbreitet, von vielen für wahr gehalten und daher an Freunde, Kollegen, Verwandte und andere Personen weitergeleitet wird. <http://de.wikipedia.org/wiki/Hoax>
Weitere Informationen z.B. unter: <http://www.cms.hu-berlin.de/dl/software/viren/hoax>

Auf dem Portal der nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) werden die Rechtsgrundlagen zum Thema «Phishing» aufgezeigt.
<http://www.cybercrime.admin.ch/content/kobik/de/home/themen/phishing.html>

Weiterführende Informationen zu den Phishing-Methoden und sicherem E-Banking bietet das nationale Portal «MELANI» (Melde- und Analysestelle Informationssicherung).
<http://www.melani.admin.ch>

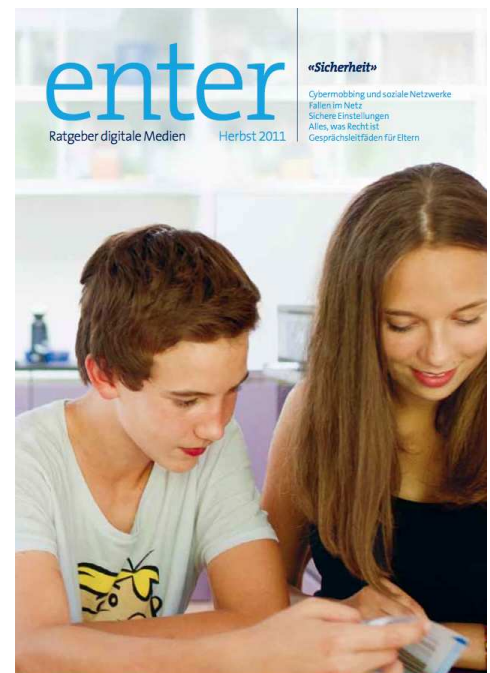
Die Swisscom bietet mit der Broschüre «enter» – Ratgeber für digitale Medien (Ausgabe Herbst 2011) eine aktuelle Übersicht zum Thema Sicherheit.

Das Heft kann gratis (als Klassensatz) unter der folgenden Adresse bezogen werden:
http://www.swisscom.ch/de/ghq/verantwortung/kommunikation-fuer-alle/jugendmedienschutz/Enter_Online_Sicherheit/bestellformular-enter.html

Der Download als PDF ist auch möglich!

Allgemeine Informationen zum Thema «Jugendmedienschutz»
<http://www.swisscom.ch/de/ghq/verantwortung/kommunikation-fuer-alle/jugendmedienschutz.html>

Weitere Links befinden sich im Anhang.





Kampagne für Persönlichkeitsschutz

Seite 4

Vorbereitung

Für die Ergänzung des Einstiegs kann die Lehrperson einen geeigneten Film im Internet (youtube, ...) suchen (s. Anhang).

Spannend wäre, eine Berufsperson einzuladen, welche sich mit Sicherheitsfragen im Internet beschäftigt. Vielleicht kommt ein Elternteil in Frage oder die betreffende Kantonspolizei verfügt über eine Fachperson, die Schulen besucht.

Die kantonalen Fachstellen können hier auch weiterhelfen.

Die Unterrichtsidee stammt aus dem Lehrmittel «Medienkompass 2» des Zürcher Lehrmittelverlages:
<http://www.lehrmittelverlag-zuerich.ch/Lehrmittel-Sites/Medienkompass/Medienkompass2/MK2Kapitel1-18/13.HierstecktderWurmdrin/tabid/687/language/de-CH/Default.aspx>

Der zum «Medienkompass 2» erhältliche Kommentar bietet der Lehrperson die Grundlagen für die Arbeit am Lesetext.



Einstieg

Zeit	Inhalte	Material
1 - 2 Lektionen	<p>Einstieg: Visionierung eines Films zum Thema (s. Anhang, weitere Beispiele im Internet: youtube, ...).</p> <p>Lesen des Textes S. 66 - 68 im «Medienkompass 2».</p> <p>Falls die Lehrperson mit kooperativen Lehr- und Lernmethoden vertraut ist, bietet sich hier die für diese Aufgabe angepasste Placemat-Methode an. Vor allem schwächere Leserinnen und Leser können hier gut abgeholt werden. http://www.kooperatives-lernen.de/dc/CL/index.html</p> <p>Auf dem Arbeitsblatt Aufgabe 1 werden die Ergebnisse zusammengetragen.</p> <p>Der Austausch der Ergebnisse erfolgt im Plenum / respektive in Form einer Präsentation (Placemat-Methode) z.B. mit Plakaten.</p>	<p>Computer mit Internet Anschluss, Beamer, Lehrmittel «Medienkompass 2» Arbeitsblatt Aufgabe 1</p>

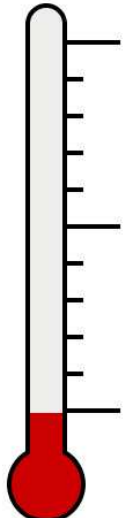


Ablauf der Unterrichtseinheit

Zeit	Inhalte	Material
1 Lektion	<p>Aufgabe 2: «E-Mail unter der Lupe»</p> <p>Die Schülerinnen und Schüler betrachten in Partnerarbeit die abgebildeten Mails und ordnen diese den drei Begriffen zu:</p> <ul style="list-style-type: none"> • Technische Gefahren • Ärgernisse • Betrügerische Aktivitäten <p>Unter «Merkmale» halten die Schülerinnen und Schüler fest, woran die entsprechenden Gefahren erkennbar sind.</p> <p>Im Plenum werden die Ergebnisse ausgetauscht.</p>	Arbeitsblatt Aufgabe 2
1 Lektion	<p>Aufgabe 3: «Eine typische Hoax-Mail»</p> <p>Die Schülerinnen und Schüler betrachten in Partnerarbeit das abgebildete Mail und markieren mit Farbe die Stellen, welche auf ein Hoax-Mail schliessen lassen.</p> <p>Im Plenum werden die Ergebnisse ausgetauscht und an der WT oder auf einem Plakat die wichtigsten Punkte festgehalten.</p>	Arbeitsblatt Aufgabe 3
Hausaufgabe	<p>Aufgabe 4: «Sicherheitscheck »</p> <p>Anhand des bisherigen Verlaufs und der formulierten Regeln können die Schülerinnen und Schüler zu Hause prüfen, welche Massnahmen eingehalten werden und welche nicht. Sie tragen ihre Ergebnisse auf dem Arbeitsblatt Aufgabe 4 ein. Schülerinnen und Schüler, die zu Hause keinen Zugang zu einem Computer haben, können die Aufgabe mit einer Mitschülerin oder einem Mitschüler erarbeiten. Es kann sinnvoll sein, den Sicherheitscheck auch anhand der Computer in der Schule durchzuführen.</p>	Arbeitsblatt Aufgabe 4



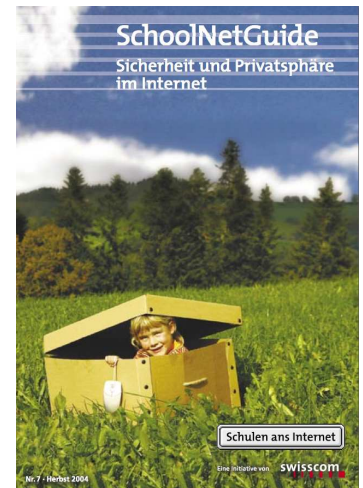
Auswertung der Resultate

Zeit	Inhalte	Material
1 Lektion	<p>Die Schülerinnen und Schüler erstellen ihr persönliches Sicherheitsprofil am Computer oder auf Papier. Sie tragen ihre wichtigsten Massnahmen zusammen und beschreiben, wie man erkennt, dass sie sich daran halten. Im Plenum werden die Profile vorgestellt und «bewertet».</p> 	<p>farbiges Papier Computer</p>



Anhang, Links

- SchoolNetGuide 7 (PDF) «Sicherheit und Privatsphäre im Internet»:
<http://www.swisscom.ch/de/ghq/schulen-ans-internet/bildungsangebote/handy-internet/schoolnetguide/sng-gesellschaft/sng-7-sicherheit.html>
- Klicksafe.de, die Plattform für Kinder, Jugendliche und Erwachsene, die umfassende Informationen zur sicheren Nutzung des Internets vermittelt. Hier zum Thema «Abzocke im Internet»:
<https://www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/index.html>
- Internet-ABC zum Thema Jugendschutz:
<http://www.internet-abc.de/eltern/gefahren-internet.php>
- Dossier von SF Wissen «Fiese Tricks im Internet»:
<http://www.sf.tv/sfwissen/dossier.php?docid=10727&navpath=med>
- PDF zum Thema «Schule, ICT und Datenschutz»:
http://www.ict-nutzung.educa.ch/dyn/bin/204472-212383-1-datenschutz_dt.pdf
- Unterrichtseinheiten auf lehrer-Online.de zum Thema «Phishing»:
<http://www.lehrer-online.de/suche.php?sid=9630622225244226331824072407710>
- Kurzerklärung «Phishing» mit Grafik:
<http://www.zeix.ch/de/lexikon/phishing>
- Mindmap zum Thema «Tipps gegen Phishing»:
http://www.mindmap.ch/gal_c0027.htm
- Information des Bundes zum Thema «Phishing»:
<http://www.melani.admin.ch/themen/00103/00203/index.html?lang=de>
<http://www.cybercrime.admin.ch/content/kobik/de/home/themen/phishing.html>
- Die Firma PayPal stellt einen dreiteiligen Phishing-Leitfaden auf ihrem Webportal zur Verfügung:
<https://www.paypal.com/at/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/UnderstandPhishing-outside>



Weitere Informationen unter:

- <http://www.microsoft.com/germany/protect/yourself/phishing/faq.msp>
- http://de.norton.com/security_response/phishing.jsp
- http://de.norton.com/clubsymantec/library/article.jsp?aid=cs_phishing_avoid_getting_hooked
- <http://themen.t-online.de/news/phishing>
- <http://www.bmelv.de/SharedDocs/Standardartikel/Verbraucherschutz/Internet-Telekommunikation/Online-Banking-Phishing.html>
- http://www.bluewin.ch/de/index.php/432,14728/Phishing_-_Betrug_im_Internet/de/digital/ratgeber/betrug
- <http://www.microsoft.com/de-de/security/online-privacy/phishing-symptoms.aspx>
- <http://www.sophos.com/de-de/security-news-trends/security-trends/online-fraud.aspx>
- <http://www.sophos.com/de-de/security-news-trends/best-practices/phishing.aspx>
- <http://www.welt.de/themen/Phishing>



Kampagne für Persönlichkeitsschutz

Seite 9

Filmbeiträge im Internet zum Thema

- YouTube: Phishing Angriff (Folge 1):
<http://www.youtube.com/watch?v=n1eaLHGxpkQ>
- YouTube: Phishing Angriff (Folge 2):
<http://www.youtube.com/watch?v=92dZbZg27O0&feature=relmfu>
- Das Schweizer Fernsehen, SF Wissen mySchool, bietet mit «Hacker, Viren, Spam & Co.» aus der Reihe «Schule und Internet» eine 15-minütige Sendung als Videostream an:
<http://www.sf.tv/sf1/myschool/detailinfo.php?docid=3263>