



## Unterrichtseinheit 10

### «Phishing»

---

Informationen zur Unterrichtseinheit .....	2
Grundlagen für die Lehrperson .....	3
Vorbereitung.....	4
Einstieg .....	5
Ablauf der Unterrichtseinheit .....	6
Auswertung der Resultate .....	7
Anhang, Links.....	8



## 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.

## Zielgruppen

Zur Zielgruppe gehören Schülerinnen und Schüler des zweiten und dritten Zyklus 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-Mails oder Kurznachrichten, um die Benutzer zu schädigen (Kontoplünderung). Der Begriff ist ein englisches Kunstwort, das sich an «password fishing» (bildlich für «Angeln nach Passwörtern mit Ködern») anlehnt.»<sup>1</sup>

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.»<sup>2</sup>

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» erläutert.

<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](http://www.swisscom.ch/de/ghq/verantwortung/kommunikation-fuer-alle/jugendmedienschutz/Enter_Online_Sicherheit/bestellformular-enter.html)

Der Download als PDF ist ebenfalls möglich.

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



<sup>1</sup> <http://de.wikipedia.org/wiki/Phishing>.

<sup>2</sup> <http://de.wikipedia.org/wiki/Hoax>



## Vorbereitung

---

Für die Ergänzung des Einstiegs kann die Lehrperson einen geeigneten Film im Internet suchen. Vorschläge finden Sie im Anhang.

Spannend wäre, eine Berufsperson einzuladen, welche sich mit Sicherheitsfragen im Internet beschäftigt. Möglicherweise kommt ein Elternteil in Frage oder die betreffende Kantonspolizei verfügt über eine Fachperson, die Schulen besucht. Die kantonalen Fachstellen können hier weiterhelfen.

Die nachfolgende Unterrichtsidee stammt aus dem Lehrmittel «Medienkompass 2» des Lehrmittelverlags Zürich. Der zum «Medienkompass 2» erhältliche Kommentar bietet der Lehrperson die Grundlagen für die Arbeit am Lesetext.<sup>3</sup>

<sup>3</sup> Medienkompass 2, Schülerbuch und Kommentar. Lehrmittelverlag Zürich. ISBN 978-3037133064 und ISBN 978-3037133071.



## Einstieg

Zeit	Inhalte	Material
1 - 2 Lektionen	<p>Einstieg: Visionierung eines Films zum Thema (Vorschläge siehe Anhang, weitere Beispiele im Internet: YouTube usw.)</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<sup>4</sup> an. Vor allem schwächere Leserinnen und Leser können damit gut abgeholt werden.</p> <p>Auf dem «Medienkompass»-Arbeitsblatt Aufgabe 1 werden die Ergebnisse zusammengetragen.</p> <p>Der Austausch der Ergebnisse erfolgt im Plenum, z.B. mit Plakaten, respektive in Form einer Präsentation (Placemat-Methode).</p>	<p>Computer mit Internet Anschluss, Beamer, Lehrmittel «Medienkompass 2», Arbeitsblatt, Aufgabe 1</p>

<sup>4</sup> Eine Beschreibung der Methode findet sich unter <http://www.kooperatives-lernen.de/dc/CL/index.html>.



## 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: Technische Gefahren Ärgernisse Betrügerische Aktivitäten</p> <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 Wandtafel oder auf einem Plakat 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 und ergänzen zur Ergebnissicherung die Merkmale der jeweiligen Massnahmen.</p> <p>Schülerinnen und Schüler, die zu Hause keinen Zugang zu einem Computer haben, können die Aufgabe mit einer Mitschülerin oder einem Mitschüler erarbeiten.</p> <p>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, auf der Basis von Aufgabe 4, ihr persönliches Sicherheitsprofil am Computer oder auf Papier.</p> <p>Im Plenum werden die Profile vorgestellt und «bewertet».</p> <div data-bbox="367 705 965 1220" style="text-align: center;"> <p><b>sehr hoher Sicherheitsstandard</b></p> <p><b>mittlerer Sicherheitsstandard</b></p> <p><b>geringer Sicherheitsstandard</b></p> </div> <p>Es ist möglich, nach 1 - 2 Monaten den «Sicherheits-Check» nochmals anzuschauen und zu überprüfen, welche Massnahmen die Schülerinnen und Schüler neu umsetzen. Die Entwicklung kann auf dem persönlichen Sicherheitsprofil abgebildet werden.</p>	<p>Farbiges Papier</p> <p>Computer</p>



## Anhang, Links

- Medienkompass 2, Schülerbuch und Kommentar. Lehrmittelverlag Zürich. ISBN 978-3037133064 und ISBN 978-3037133071.
- 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>
- Unterrichtseinheiten auf Lehrer-Online.de zum Thema «Phishing»:  
<http://www.lehrer-online.de/phishing-mail.php?sid=41163300308335980937846854685820>
- Kurzerklärung «Phishing» mit Grafik:  
<http://www.zeix.ch/de/lexikon/phishing>
- 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/security_response/phishing.jsp)
- [http://de.norton.com/clubsymantec/library/article.jsp?aid=cs\\_phishing\\_avoid\\_getting\\_hooked](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.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>

### 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>