Idee e suggerimenti per la lezione

«Parte 10: Phishing»

Istituto per l'aggiornamento e la consulenza
Sezione Argovia

Küttigerstrasse 42
5000 Aarau

T +41 62 838 90 32
F +41 62 838 90 09

joerg.graf@fhnw.ch
www.fhnw.ch

Informazioni sull’unità didattica

Questa unità didattica si occupa del «Phishing». Serve per sensibilizzare gli alunni su questo argomento e fare in modo che elaborino e interiorizzino comportamenti prudenti da adottare nel tempo libero e a scuola.
Assieme al «Medienkompass 2» della Lehrmittelverlag di Zurigo rappresenta un supporto didattico adeguato, che può essere utile a tutti i docenti.

Destinatari

Docenti e alunni delle scuole medie e superiori di età compresa tra i 10 e i 14 anni.

Modalità di lavoro e tempistiche

Gli alunni lavorano a livello di gruppo classe, in piccoli gruppi e da soli o in coppia al computer. È utile avere a disposizione una connessione Internet.

Obiettivi didattici

Agli alunni viene fornita una panoramica sull'argomento «Sicurezza – pericoli esterni in Internet».
Gli alunni imparano a riconoscere alcune forme di «phishing».
Gli alunni imparano che devono comportarsi in modo da garantire la propria sicurezza quando navigano in Internet.

Istituto per l’aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch

Conoscenze di base per il docente

Ecco come la versione in tedesco di Wikipedia descrive il «Phishing»: si chiama phishing il tentativo di accedere ai dati degli utenti di Internet, ad es. tramite indirizzi Internet contraffatti, e-mail o messaggi brevi, con lo scopo di danneggiare l'utente (furto dell'account). La parola è un neologismo inglese, derivato da «password fishing» (metaforicamente «pescare password con l'inganno») http://de.wikipedia.org/wiki/Phishing

Ecco come la versione in tedesco di Wikipedia descrive il cosiddetto «Hoax»: Per hoax (ingl. per scherzo, burla) s'intende un messaggio contraffatto diffuso su libri, riviste, giornali, e-mail, instant messenger o altri supporti (ad es. SMS, MMS o social network), che molte persone considerano autentico e quindi inoltrano a colleghi, amici e conoscenti. http://de.wikipedia.org/wiki/Hoax
Per ulteriori informazioni, è possibile consultare: http://www.cms.hu-berlin.de/dl/software/viren/hoax

Il portale del Servizio di coordinazione per la lotta alla criminalità su Internet (SCOCI) riporta la legislazione relativa al «Phishing».
http://www.cybercrime.admin.ch/content/kobik/it/home/themen/phishing.html

Per ulteriori informazioni sulle tecniche di phishing e la sicurezza dell'e-banking, è possibile consultare il portale della Centrale d'annuncio e analisi per la sicurezza dell'informazione «MELANI».
http://www.melani.admin.ch

Per una panoramica sull'uso sicuro dei media digitali è possibile consultare la guida «enter» (ed. autunno 2011) di Swisscom.

L'opuscolo è gratuito e può essere utilizzato in classe. La richiesta può essere effettuata all'indirizzo:
http://www.swisscom.ch/it/ghq/responsabilita/comunicazione-per-tutti/tutela-dei-giovani-dai-media/enter-online-sicurezza/bestellformular-enter.html

L'opuscolo può anche essere scaricato in formato PDF!

Informazioni generali sulla tutela dei giovani dai media
http://www.swisscom.ch/it/ghq/responsabilita/comunicazione-per-tutti/tutela-dei-giovani-dai-media.html

Ulteriori link in allegato.

Istituto per l'aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch

Preparazione

Per integrare la fase di warm up, i docenti possono cercare su Internet un filmato adeguato (ad es. su youtube). In allegato sono presenti alcune indicazioni in proposito.

È anche possibile invitare un esperto specializzato nella sicurezza su Internet. Forse si possono anche coinvolgere i genitori o la polizia cantonale ha personale disposto a collaborare con la scuola. Ulteriore supporto può venire dalle associazioni cantonali.

L'unità didattica si basa sul testo «Medienkompass 2», Lehrmittelverlag, Zurigo.
http://www.lehrmittelverlag-zuerich.ch/Lehrmittel-Sites/Medienkompass/Medienkompass2/MK2Kapitel1-18/13.HierstecktderWurmdrin/tabid/687/language/de-CH/Default.aspx

Il commento a «Medienkompass 2» contiene anche utili indicazioni didattiche.

Istituto per l'aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch

Warm up

Tempistiche	Contenuti	Materiali
1 - 2 lezioni	Warm up: proiezione di un filmato sull'argomento (vedi allegati, ulteriori esempi in Internet: youtube, ...). Lettura del testo a pag. 66 - 68 di «Medienkompass 2». Se il docente è abituato a utilizzare metodi di apprendimento cooperativo, può utilizzare una versione adattata del metodo placemat, che consente di coinvolgere in modo adeguato gli alunni con competenze di lettura più deboli. http://www.kooperatives-lernen.de/dc/CL/index.html I risultati vanno riportati sul foglio di lavoro relativo al compito 1. La condivisione dei risultati avviene con tutto il gruppo classe o in forma di presentazione (metodo placemat), ad es. con cartelloni.	Computer con connessione Internet, beamer, «Medienkompass 2» Foglio di lavoro per il compito 1

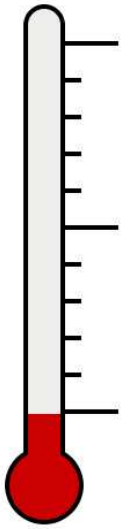
Istituto per l'aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch

Svolgimento dell'unità didattica

Tempistiche	Contenuti	Materiali
1 lezione	Compito 2: «E-Mail al microscopio» Gli alunni lavorano in coppia, analizzano le e-mail e le classificano nelle tre seguenti categorie: • Pericoli di tipo tecnico • Seccature • Attività fraudolente Nella parte «Caratteristiche» devono indicare gli aspetti che consentono di riconoscere il pericolo insito nelle diverse e-mail. I risultati vengono condivisi con tutto il gruppo classe.	Foglio di lavoro per il compito 2
1 lezione	Compito 3: «Un esempio tipico di e-mail con hoax» Gli alunni lavorano in coppie, analizzano l'e-mail ed evidenziano i punti che consentono di classificarla come hoax mail. I risultati vengono condivisi con tutto il gruppo classe e i punti principali vengono fissati alla lavagna o in un cartellone.	Foglio di lavoro per il compito 3
Compito domestico	Compito 4: «Controllo della sicurezza» A partire da quanto hanno appreso, gli alunni sono in grado di verificare a casa propria quanto sicure sono le impostazioni del loro computer. Devono inserire i risultati nel foglio di lavoro per il compito 4. Gli alunni che a casa non hanno un computer possono svolgere il compito con un compagno o una compagna. È una buona idea svolgere l'attività anche su uno dei computer presenti a scuola.	Foglio di lavoro per il compito 4

Istituto per l'aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch

Valutazione dei risultati

Tempistiche	Contenuti	Materiali
1 lezione	Gli alunni elaborano il proprio profilo di sicurezza personalizzato al computer o su carta. Elencano le principali misure di sicurezza e descrivono come è possibile verificare che siano applicate correttamente. I profili vengono presentati e «valutati» con tutto il gruppo classe.  **Grado di sicurezza molto elevato** **Grado di sicurezza medio** **Grado di sicurezza basso**	Carta colorata Computer

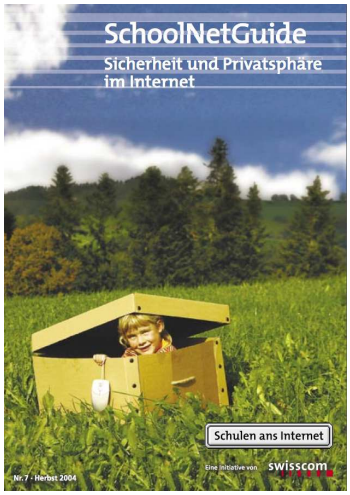
Istituto per l'aggiornamento e la consulenza
Sezione Argovia

Küttigerstrasse 42
5000 Aarau

T +41 62 838 90 32
F +41 62 838 90 09

joerg.graf@fhnw.ch
www.fhnw.ch

Allegati, link



- SchoolNetGuide 7 (PDF) «Sicurezza e sfera privata in Internet»: http://www.swisscom.ch/it/ghq/scuole-in-internet/offerte-di-formazione/cellulare-internet/schoolnetguide/sng-societa/sng-7-sicurezza.html

- Klicksafe.de (in tedesco), la piattaforma per bambini, ragazzi e adulti con informazioni complete sull'utilizzo sicuro di Internet. Qui, sull'argomento «Truffe in Internet»: https://www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/index.html

- L'ABC di Internet relativamente alla protezione dei minori (in tedesco): http://www.internet-abc.de/eltern/gefahren-internet.php

- Servizio (in tedesco) della trasmissione SF Wissen «Brutti tiri su Internet»: http://www.sf.tv/sfwissen/dossier.php?docid=10727&navpath=med

- PDF «Scuola, ICT, protezione dati»: http://insegnamento.educa.ch/sites/default/files/20110329/educa.dossier_scuola%20e%20protezione%20dati.pdf

- Unità didattiche (in tedesco) sul «phishing» disponibili su lehrer-Online.de: http://www.lehrer-online.de/suche.php?sid=96306222225244226331824072407710

- Breve definizione di «phishing» con grafico (in tedesco e francese): http://www.zeix.ch/de/lexikon/phishing

- Mappa mentale «Consigli per combattere il phishing» (in tedesco): http://www.mindmap.ch/gal_c0027.htm

- Informazioni delle autorità federali sul «phishing»: http://www.melani.admin.ch/themen/00103/00203/index.html?lang=it http://www.cybercrime.admin.ch/content/kobik/it/home/themen/phishing.html

- Informazioni sul «phishing» sul portale web di PayPal: https://cms.paypal.com/it/cgi-bin/marketingweb?cmd=_render-content&content_ID=security/security_protection&locale.x=it_IT#phishing-recognize

  Per ulteriori informazioni, è possibile consultare:
  http://www.microsoft.com/it-it/security/online-privacy/default.aspx#Frode
  it.norton.com/security_response/phishing.jsp
  http://it.norton.com/clubsymantec/library/article.jsp?aid=cs_phishing_avoid_getting_hooked
  http://themen.t-online.de/news/phishing (in tedesco)
  http://www.bmelv.de/SharedDocs/Standardartikel/Verbraucherschutz/Internet-Telekommunikation/Online-Banking-Phishing.html (in tedesco)
  http://www.bluewin.ch/it/index.php/472,17050/?campID=src_phishing%20internet
  http://www.microsoft.com/it-it/security/online-privacy/phishing-symptoms.aspx
  http://www.sophos.com/it-it/security-news-trends/security-trends/online-fraud.aspx
  http://www.sophos.com/it-it/security-news-trends/best-practices/phishing.aspx
  http://www.welt.de/themen/Phishing (in tedesco)

Istituto per l'aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch

Filmati disponibili in Internet

- YouTube: Phishing Angriff (in tedesco) – parte 1:
  http://www.youtube.com/watch?v=n1eaLHGxpkQ

- YouTube: Phishing Angriff (in tedesco) – parte 2:
  http://www.youtube.com/watch?v=92dZbZg27O0&feature=relmfu

- Il programma della televisione svizzera SF Wissen mySchool mette a disposizione in modalità streaming una trasmissione di 15 minuti della serie «Scuola e Internet» intitolata «Hacker, Virus, Spam & Co.» (in tedesco).
  http://www.sf.tv/sf1/myschool/detailinfo.php?docid=3263

Istituto per l'aggiornamento e la consulenza
Sezione Argovia
Küttigerstrasse 42
5000 Aarau
T +41 62 838 90 32
F +41 62 838 90 09
joerg.graf@fhnw.ch
www.fhnw.ch