Ich bin online :(

Pädagogisch-didaktische Begleitinformation

LKA SACHSEN-ANHALT

Inhalt der DVD

Diese DVD beinhaltet:

1. Video-DVD mit dem Projekt (über DVD-Player)

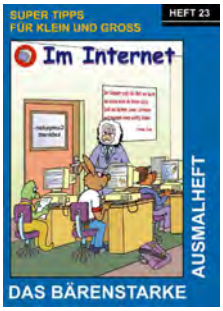
2. Begleitmaterial zum Thema:

- Pädagogisch-dikaktische Begleitinformation mit Unterrichtseinheiten und entsprechenden Arbeitsmaterialien

- Flyer „Skimming“

- Flyer „Phishing“

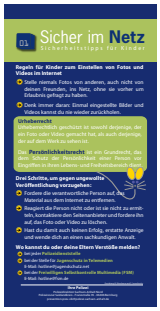
- Malhefte:
  Heft 23 „Im Internet“



- Heft 28 „Mein Handy ist okay“

- Projektinitiative „Sicher im Netz“ von Bettina Moosbauer
  Sachbearbeiterin Prävention
  Polizeiliche Information und Beratung
  Polizeirevier Salzlandkreis
  Franzstraße 35
  06406 Bernburg

mit: Lesezeichen „Sicher im Netz“
Schreibunterlage „Sicher chatten“
Handouts: „Sicher im Netz – Kinder“
„Sicher im Netz – Eltern“
„Ungewollt im www“



Inhalt

Kinder

Jugendliche

Jugendliche

Erwachsene

Musikvideo

Tipps

Soziale Netzwerke

Angie erklärt: Soziale Netzwerke

Das sind Julia und Svenja. Die beiden haben sich in den Sommerferien im Urlaub an der Ostsee kennengelernt und sind seitdem unzertrennlich. Leider wohnen sie über 400 km voneinander entfernt.

Zum Glück gibt es Internet und so können sie auf verschiedenen sozialen Netzwerken im Internet miteinander kommunizieren. Auf studiVZ und facebook sind beide angemeldet. Sie nutzen die Plattform, um sich zu schreiben. Sie schicken sich gegenseitig Fotos, die sie geschossen haben. Sie stellen ihre Lieblingsmusik rein, pflegen ihre Freundschaftsliste und geben Kommentare und Bewertungen auf anderen Seiten ab. Auch Chats und Foren gehören zu den sozialen Netzwerken, die sie beide benutzen. Sie bewegen sich wie in einem normalen Freundeskreis voller Vertrauten.

Doch das täuscht. Im Internet lauern unterschiedliche Gefahren. Umso mehr Menschen über Julia oder Svenja etwas wissen, desto angreifbarer machen sie sich. Das Offenlegen persönlicher Daten (wie zum Beispiel E-Mail-Adresse, Telefonnummern etc.) kann von Firmen missbraucht werden, die die beiden zum Beispiel mit Werbung bombardieren. Darum ist es Julia und Svenja auch wichtig, dass nur ihre Freunde ihr ganzes Profil sehen können, für andere ist dies nicht möglich. Auch mögliche zukünftige Chefs von Julia und Svenja können somit nicht sehen, was die beiden so in ihrer Freizeit treiben.

Was gibt es noch für Gefahren in den sozialen Netzwerken? Eine Gefahr im Internet ist das „Phishing". Über gefälschte Webseiten versuchen Betrüger an die Zugangsdaten für eure Netzwerkkonten zu kommen. Die Links zu diesen gefälschten Webseiten sind oft täuschend echt. Wenn ihr euch da einloggen würdet, hätten die Betrüger alle eure Kontaktdaten und könnten, ohne dass ihr etwas davon mitbekommen würdet, euren Freunden irgendwas schreiben.

Aber nicht nur das, es gibt auch Identitätsdiebstahl. Das geht noch eine Stufe weiter. Sogenannte Hacker knacken deinen Account und bitten deine Freunde um finanzielle Hilfe, indem sie angeben, dass man in Gefahr, schwer krank oder irgendwo auf der Welt verloren gegangen ist. Die Betrüger spielen somit mit den Gefühlen deiner Freunde und Familie.

Als dritten Missbrauch ist das Mobbing zu nennen. Das ist eine besonders schlimme Sache, die Julia und Svenja am eigenen Leib erfahren haben. Im Internet werden schneller Freundschaften über soziale Netzwerke geschlossen, als im wahren Leben. Die „echten" Freunde prüft man oft auf Herz und Nieren. Im Internet gelangen viele Informationen an viele Leute, die sie vielleicht gegen dich verwenden. Man kann sich nicht davor schützen, beschimpft oder beleidigt zu werden, da das Netz so anonym ist. Der Unbekannte, der dort beleidigt, hat meist nicht mit Konsequenzen zu rechnen. Selbst bei Bekannten von dir kann durch diese vermeintliche Anonymität die Hemmschwelle schnell sinken.

Auch innerhalb der sozialen Netzwerke ist es wichtig, nicht alles zu glauben, schon gar nicht, wenn Nachrichten zum Beispiel bei facebook, mit einem Link versehen, bei euch eingehen. Es kann sich dabei um manipulierte Webseiten handeln, die darauf angelegt sind, Schadsoftware zu vertreiben. Damit sind unter anderem Viren oder Trojaner gemeint. Auch müsst ihr vorsichtig sein bei Zusatzanwendungen, zum Beispiel bei Mini-Spielen, die ihr eurem Profil zufügen könnt. Oftmals stammen diese Spiele von Drittanbietern, deren Sicherheitsstandards nicht unbedingt die der sozialen Netzwerke entsprechen müssen.

Julia und Svenja fühlen sich wohl und sicher bei facebook, studiVZ und Co., weil sie es vor allem für ihre Freundschaft machen. Sie nehmen nur neue Freunde auf, über die sie sich vorher schon informiert haben. Intime Sachen und Fotos werden nur über private E-Mails ausgetauscht. Sollte es zu dauerhafter Belästigung eines „virtuellen" Freundes kommen, würden sie sich nicht scheuen, diese Information an Zuständige weiterzuleiten. Auch wenn es nicht so bequem ist, so haben sich Julia und Svenja für unterschiedliche Passwörter auf ihren Seiten entschieden, damit sie vor Angriffen geschützter sind.

Soziale Netzwerke – Unterrichtseinheit

Gefahren im Umgang mit dem Internet

Zielgruppe: ab Klasse 3

Dauer: 4 – 5 Zeitstunden

Lernziele:

- Die Schülerinnen und Schüler reflektieren ihre eigene Medienausstattung und Mediennutzung. Sie setzen sich mit den Meinungen der Mitschüler zum Medienumgang auseinander.

- Die Schülerinnen und Schüler schauen ein Puppenspiel zum Thema „Soziale Netzwerke“ und fassen die Inhalte in einem Gespräch zusammen.

- Die Schülerinnen und Schüler beschäftigen sich mit der gesehenen Geschichte und versuchen die Geschichte umzuschreiben, ihr ein neues Ende zu geben.

Materialien:

Tafel, Kreide, Mediensymbole, Kartenabfrage, Puppenspiel, „Fragen und Tipps für groß und KLEIN – Soziale Netzwerke“, Leinwand, Beamer, PC,

Methoden:

Einzelarbeit, Partnerarbeit, Gruppenarbeit, Gesprächskreis

Unterrichtsplanung:

Als Einstieg in die Thematik bietet es sich an, die Mediennutzung, insbesondere die Internetnutzung der Kinder, zu erfahren. Dafür können die Mediensymbole verwendet werden (Material 1). Es werden alle Mediensymbole einmal hochgehalten und die Kinder sollen sich in einer Reihe vor der Lehrkraft aufstellen. Die Kinder müssen dabei untereinander Absprachen treffen, wie lange sie dieses Medium in der Woche nutzen. Das Kind, das ganz vorn steht, hat die höchste Nutzungsdauer, das Kind am Ende der Schlage die niedrigste Nutzungsdauer.

Daran schließt sich eine Kartenabfrage an, bei der Sie gut die Meinungen der Kinder zum Thema erfragen können (Material 2). Jedes Kind bekommt einen Stapel mit Karten, auf denen verschiedene Aussagen zur Internetnutzung stehen. Sie sollen sich die Aussagen durchlesen und jeder entscheidet für sich, ob es dieser zustimmt oder diese ablehnt. Es werden zwei Stapel gebildet. Wenn alle die Karten für sich geordnet haben, werden diese auf den Boden gelegt. In der Mitte hat die Lehrkraft die Zettel mit den Buchstaben in einer anderen Farbe untereinander ausgelegt. Links und rechts daneben wird jeweils ein lachender und ein weinender Smily ausgelegt. Dann ordnen die Schülerinnen und Schüler ihre Karten den Smilys zu. Die A-Zustimmungskärtchen in eine Reihe, darunter die B-Zustimmungskärtchen usw. Das Gleiche auch für die Meinungen denen sie nicht zugestimmt haben. Über die entstandenen Balkendiagramme kann diskutiert werden. Welche Meinungen wurden überwiegend abgelehnt und welchen wurde überwiegend zugestimmt. Welche Gründe geben die Schülerinnen und Schüler für ihre Entscheidung an.

Nun schauen sich die Schülerinnen und Schüler das Puppenspiel aufmerksam an. Anschließend wird das Gesehene in einem Gesprächskreis ausgewertet. Mögliche Fragen für die Lehrkraft: Wer war zu Beginn des Puppenspiels zu sehen? Was hat das Schaf gemacht? Welche Daten hat das Schaf von sich preisgegeben? Mit wem hat es sich verabredet? Wen hat das Schaf im Park getroffen? Was hat das Schaf gemacht, als es beklaut wurde? Wie wurde die Geschichte aufgelöst?

Im nächsten Schritt werden die Schülerinnen und Schüler gebeten, die gesehene Geschichte umzuschreiben. Was wäre passiert, wenn das Schaf den Fernsehbeitrag nicht gesehen hätte? Wie wäre dann die Geschichte ausgegangen? Zuerst werden Ideen an der Tafel gesammelt und die Schülerinnen und Schüler in Vierergruppen eingeteilt. Anschließend werden in den Gruppen die Ideen vertieft und erste Notizen angefertigt. Für die Fertigstellung der neuen Geschichte wird eine weitere Unterrichtsstunde benötigt.

Soziale Netzwerke – Unterrichtseinheit

Zum Abschluss zeigt die Lehrkraft den Schülerinnen und Schülern den Film „Fragen und Tipps für groß und KLEIN“. Darin werden Verhaltensregeln für das Internet in einem Frage-/Antwortszenario für die Jüngsten anschaulich dargestellt. Diese Verhaltensregeln werden aufgeschrieben und daraus wird eine Wandzeitung für den PC-Raum gestaltet, sodass mehrere Kinder davon profitieren. In die Gestaltung fließen auch selbstgemalte Bilder von den Kindern mit ein.

Hausaufgabenvorschlag:

Die Schülerinnen und Schüler gestalten Bilder, die inhaltlich und thematisch zu den Verhaltensregeln auf der Wandzeitung passen.

Alternativ für die größeren Kinder:

Die Schülerinnen und Schüler haben die Aufgabe, am Nachmittag zusammen mit ihren Eltern den Kinderchat www.seitenstark.de/chat zu besuchen und ihn auszuprobieren.

Jedes Kind erstellt eine Liste mit dem, was ihm aufgefallen ist. Darüber kann im Unterricht gesprochen werden.

Soziale Netzwerke

Material 1

Mediensymbole

Fernseher 
Radio 
Computer 
Handy 
Print 
Spielekonsole 

Die Mediensymbole befinden sich auf der DVD im DIN A4-Format.

Material 2

Kartenabfrage

Die Karten vervielfältigen und ausschneiden.

Kindern sollte der Zugang zum Internet auf 4 Stunden in der Woche begrenzt sein! A	Soziale Netzwerke und Chats sind klasse, Gott sei Dank haben Erwachsene dort keinen Zugriff. D
So schlimm sind die Gefahren im Internet gar nicht, die Erwachsenen übertreiben nur. B	Es ist gut, dass sich Kinder früh mit dem Computer beschäftigen, das ist für das ganze Leben wichtig. E
Wer im Internet gemobbt wird, ist selber daran schuld. C	Seit dem ich im Internet in sozialen Netzwerken angemeldet bin, habe ich mehr Freunde als früher. F

Online-Banking

Angie erklärt: Online-Banking

Das ist Tim. Tim ist neuerdings Verkäufer in einem Sportgeschäft.

Um seine Ersparnisse zu verwalten, hat er ein Konto bei einer Bank eröffnet.

Weil er oft lange arbeiten muss und keine Lust hat, immer zur Bank zu fahren, macht Tim jetzt Online-Banking. Bequem im Internet von zu Hause aus.

Er kann Überweisungen oder Daueraufträge durchführen, bei „ebay" einen neuen Fußball kaufen oder einfach nur seinen Kontostand abfragen.

Dafür muss er sich nur von der Bank Zugangsdaten für sein persönliches Onlinekonto zukommen lassen.

Hierbei steht die Sicherheit an höchster Stelle, denn im Internet gibt es viele Betrüger und Kriminelle, die sich nur darauf spezialisiert haben, Kontodaten und Kreditkartendaten rauszufischen, um so zum Beispiel an das Geld von Tim ranzukommen.

Darum verwenden die Banken als Verbindungssystem für das Online-Banking das verschlüsselte SSL (Secure Sockets Layer), um mehr Sicherheit zu gewährleisten.

Dies erkennt man daran, dass die URL mit „https" statt „http" beginnt.

Tim bekommt von der Bank außerdem noch persönliche Zugangsdaten, die meist über das Pin/Tan-System erfolgen. Dabei muss Tim, neben seiner Kontonummer auch eine persönliche Identifikationsnummer (PIN) eingeben. Zu guter Letzt braucht er noch eine Transaktionsnummer (TAN) um den Vorgang auszuführen. Es gibt aber verschiedene Arten, eine Transaktion durchzuführen.

Die iTan ist eine davon. Dabei sind verschiedene Transaktionsnummern (TAN) auf einer Liste durchnummeriert. Und wenn dann eine Transaktion erfolgt, wird eine bestimmte Nummer auf der TAN-Liste abgefordert, die dann mit dem aktuellen Auftrag gebunden ist.

Eine weitere Möglichkeit der bequemen Transaktion bietet mTAN oder SMSTAN. Hier gibt es keine TAN-Liste, sondern man erhält bei jeder Transaktion eine „mobile TAN" als SMS aufs Handy geschickt. Diese TANs müssen umgehend genutzt werden, sonst verfallen sie.

Die dritte Möglichkeit ist das chipTAN-Verfahren. Hier erhält Tim von seiner Bank einen TAN-Generator mit Ziffernfeld und Karteneinschub, auf dessen Rückseite zusätzlich fünf optische Sensoren angebracht sind. Wenn Tim jetzt Geld überweisen will, erscheint auf dem Bildschirm eine Grafik mit fünf flackernden schwarzweißen Flächen. Dann muss er seine Bankkarte in den TAN-Generator stecken und diesen an die Grafik auf dem Monitor halten. Durch diese Lichtsignale werden alle nötigen Informationen an den Generator übertragen, der nun eine TAN errechnen kann.

Tim kann nun richtig loslegen und doch muss er immer auf die Sicherheit achten.

Folgende Regeln hält er ganz besonders ein:

- Er wählt ein schwieriges Passwort aus vielen Buchstaben und Zahlen, das man nicht so einfach knacken kann.
- Tim benutzt auch immer eine aktuelle Virenschutzsoftware und aktiviert seine Firewall.
- Tim hat eine Vereinbarung mit der Bank getroffen, dass es ein Limit für tägliche Geldbewegungen gibt. Somit kann das Konto nicht ungeschützt überzogen werden.
- Er antwortet nicht auf E-Mails, in denen er aufgefordert wird, seine Kontodaten zu aktualisieren.
- Er sperrt sofort seinen Online-Banking-Zugang, wenn ihm etwas verdächtig vorkommt.

Phishing

Angie erklärt: Phishing

Das ist Jochen. Bei Jochen hängt der Haussegen schief. Jochen sitzt gerade am Telefon und telefoniert mit seiner Bank. Er ist dabei sehr aufgeregt. Denn seitdem Jochens Frau, Johanna, gestern früh eine E-Mail geöffnet hat und aufgefordert wurde, ihre Zugangsdaten für ihren Online-Banking-Account freizulegen, fehlt Geld auf ihrem gemeinsamen Konto.

Wie konnte das passieren? Die Bank glaubt, dass Johanna ein „Phishing-Opfer" geworden ist. „Phishing" kommt von „fishing", was soviel wie „Fischen" oder „Angeln" bedeutet.

Im Internet heißt das nichts anderes als Datendiebstahl. Dabei wird versucht, an sensible Daten wie Passwörter und PIN-Nummern zu gelangen. Die Betrüger gehen dabei oft in Gruppen vor und nutzen diese geheimen Daten, um an die Kohle ihrer Opfer ranzukommen. Das geschieht zum Beispiel über gefälschte E-Mails und Webseiten.

Der erste Schritt der Täter ist nämlich massenweise E-Mails zu versenden, um damit ein Vertrauensverhältnis mit den Opfern aufzubauen. In diesen E-Mails stehen oft weiterführende Links, die auf gefälschte Webseiten führen wie zum Beispiel zu der gefälschten Webseite der Bank von Johanna und Jochen. Diese manipulierten Webseiten sind von den Originalen kaum zu unterscheiden. Nur Aufmerksame können erkennen, dass die Adressen abweichen und dass diese manipulierten Seiten kein gültiges Sicherheitszertifikat aufweisen.

Johanna fragt Jochen, was sie tun kann, damit so was nicht noch einmal passiert. Jochen sagt, dass sie nie wieder einfach so ihre vertraulichen Daten angeben soll. Ein seriöses Unternehmen, wie ihre Bank, würde sie nie auffordern, solche Daten per Mail oder Telefon preiszugeben.

Und aufgepasst: „Phishing" gibt es nicht nur im Internet in Form von E-Mails. Auch „Voice-Phishing" oder „SMiShing" (SMS-Phishing) gibt es. Hier gehen die Betrüger noch dreister vor und versuchen in einem persönlichen Telefonat oder SMS an die vertraulichen Daten ranzukommen.

Jochen bleut Johanna auch ein, dass sie sich jetzt immer eine E-Mail im Rein-Text-Format anzeigen lassen soll, denn HTML-E-Mails lassen sich leicht manipulieren. Oft sind „Phishing-Texte" auch nicht einwandfrei zu lesen. Damit sind zum Beispiel kyrillische Zeichen gemeint, die sich in den Text einschleichen oder anstatt einem „ä" wird ein „a" oder „ae" angezeigt. Jochen bittet Johanna auch, nur E-Mail-Anhänge von Leuten zu öffnen, die sie kennt und denen sie vertraut.

Die Bank gibt auch noch ein paar Tipps mit auf den Weg und rät Jochen und Johanna, für jede Anwendung ein anderes Passwort anzulegen und weist sie auf das Sicherheitszertifikat hin. Dieses Sicherheitszertifikat zeigt an, ob man wirklich mit einer sicheren Webseite verbunden ist. Diese erkennt man immer an einem grün/blauen Feld mit Zertifikats- und Domaininhaber in der Adressleiste und einem Schlosssymbol in der Statusleiste im Browser.

Auch sollen Johanna und Jochen darauf achten, dass beim Eingeben vertraulicher Daten die Verbindung verschlüsselt ist, meist wird dabei der Standard SSL verwendet („https").

Phishing erkennt man auch an kleinen Adressabweichungen. Zum Beispiel an einem Zusatz wie beim folgenden Beispiel: www.deutsche-bankXY.de. Zu guter Letzt rät die Bank Jochen, die Software wie Antivirenprogramme, Firewall, Betriebssystem und Browser immer auf dem aktuellen Stand zu haben.

Als letzten Schritt muss Jochen noch die Polizei anrufen. Er erstattet Anzeige: gegen Unbekannt.

Online-Shopping

Angie erklärt: Einkauf im Internet

Das ist Lisa. Lisa liebt shoppen. Sie könnte es den ganzen Tag, 24 Stunden, sieben Tage die Woche machen. Lisa lebt in einer Kleinstadt und findet die Klamottenläden dort alle öde. Darum hat sie die „Onlineshops" für sich entdeckt.

Fast jedes Kaufhaus bietet heute die Möglichkeit an, Sachen über das Internet zu kaufen. Und da Lisa ein alter Hase ist, kennt sie sich auch mit den speziellen Zahlungsmöglichkeiten bestens aus.

Eine Variante sind die „Prepaid-Karten". Diese funktionieren wie Telefonkarten mit Guthaben. Man rubbelt auf der Karte einen PIN-Code frei und kann somit auf der Internetseite des jeweiligen Händlers auf das Guthaben zugreifen. Ein großes Plus dabei – man braucht dafür kein Passwort.

„PayPal" ist die zweite Möglichkeit und bedeutet, dass man ein virtuelles Konto anlegen kann, worüber dann alle Geschäfte und Einkäufe laufen. Lisa kann ihr „PayPal-Konto" später wieder über eine Kreditkarte oder eine Lastschrift ausgleichen.

Zu guter Letzt gibt es da noch die Sammelrechnung. Bei der Firma „Firstgate" kann man sich ein sogenanntes „Surfer-Konto" einrichten, dafür muss man aber persönliche Daten wie Name, Wohnort, Bankverbindung und E-Mail-Adresse angeben.

Doch auch bei Lisa gilt bei all dem Spaß die goldene Regel: Lieber mehr Zeit in das Lesen der allgemeinen Geschäftsbedingungen investieren, als sich hinterher zu ärgern.

Eine große Gefahr beim Einkauf im Internet ist natürlich die Kriminalität. Wenn dir zum Beispiel jemand eine E-Mail schreibt und dich auffordert, deine persönlichen Daten zu aktualisieren, lösche die E-Mail schnell! Meist handelt es sich dabei um eine dubiose Aufforderung und hat einzig und allein den Zweck, an deine persönlichen Daten ranzukommen und dir finanziellen Schaden zuzufügen.

Darum achtet Lisa immer darauf, dass es sich um einen seriösen Anbieter handelt. Eindeutige Indizien dafür sind, dass neben den elektronischen Kontaktdaten auch Adresse und Telefonnummern angegeben werden. Du solltest keine Passwörter, PIN, TAN oder andere Zugangscodes auf deinem Rechner speichern. Vor allem nicht zusammen an einem Ort. Lisa verzichtet außerdem auf das Ausführen „aktiver Inhalte" und stellt ihren Browser auch so ein, dass Java Script nicht automatisch ausgeführt werden kann. Außerdem aktualisiert und benutzt sie beim Surfen im Internet immer eine Firewall und ein Virenschutzprogramm.

Und jetzt viel Spaß beim Shoppen!

Online-Shopping – Unterrichtseinheit

Schwerpunkt: Klingelton – Abofalle

Zielgruppe: ab Klasse 3

Dauer: 3 Zeitstunden

Lernziele:

- Die Schülerinnen und Schüler werden für die Problematik der Abofallen sensibilisiert.

- Die Schülerinnen und Schüler lernen sich kritisch mit diesem Thema auseinanderzusetzen und sie bekommen Verhaltensregeln für den Einkauf im Internet an die Hand, um Risiken besser erkennen zu können.

Methoden:

Einzelarbeit, Gruppenarbeit

Materialien:

Ein großes Papier (z. B. Tapete), Stifte, Beamer, Laptop, Leinwand, Puppenspiel „Teure Töne“, „Fragen und Tipps für groß und KLEIN – Einkaufen im Internet“

Unterrichtsplanung:

Zu Beginn der Unterrichtseinheit schreibt die Lehrkraft das Wort „Handy“ groß und deutlich auf ein großes Stück Papier, malt noch ein Telefon daneben und fragt die Schülerinnen und Schüler: „Was fällt euch ein, wenn ihr an ein Handy denkt?“ Die Schülerinnen und Schüler nennen ihre Assoziationen. Die Lehrkraft oder die Kinder selber schreiben ihre Ideen auf das Poster rund um das Wort in der Mitte. Abhängig von den Ideen kann die Lehrkraft nachfragen, weitere Überlegungen anregen oder ergänzen. (Mögliche Fragen: Wer besitzt ein eigenes Handy? Welche Funktionen werden genutzt? Wie viel Guthaben steht jedem zur Verfügung? Welche Gefahren im Umgang mit dem Handy kennen die Kinder?)

Danach schauen sich die Schülerinnen und Schüler das Puppenspiel „Teure Töne“ gemeinsam an. Im Anschluss wird in einem Sitzkreis das Gesehene wiederholt und ausgewertet. (Möglich Fragen könnten sein: Wo hat Steffi Bär die Werbung mit dem Klingelton gesehen? Kennen die Kinder Klingeltonwerbung im Fernsehen? Gibt es ein Kind, das schon einmal solche Klingeltöne gekauft hat? Mit welchen Gefahren ist dort zu rechnen? Gibt es von den Eltern Bestrafungen (Handy- oder Fernsehverbot), wenn etwas nicht oder falsch gemacht wurde? (z. B. nicht Aufräumen, Unpünktlichkeit)

Die Gefahren lauern jedoch nicht nur beim Kauf von Klingeltönen oder Handylogos. Es gibt verschiedene Risiken auf die die Schülerinnen und Schüler aufmerksam gemacht werden müssen. Gleichzeitig erhalten sie dazu Handlungsempfehlungen, um in der jeweiligen Situation richtig zu reagieren. Dazu schauen sie sich gemeinsam das Video „Fragen und Tipps für groß und KLEIN – Einkaufen im Internet“ an, um einen ersten Eindruck zu bekommen. Hier werden verschiedene Bereiche angesprochen, in denen Vorsicht geboten ist. Um die Inhalte besser zu verstehen und gemeinsam durchzuarbeiten, lesen die Kinder das Gesagte auf dem Arbeitsblatt 1 noch einmal nach. Die Schülerinnen und Schüler sollen die wichtigsten Verhaltensregeln auf einer Checkliste zusammenfassen.

Folgende Bereiche werden im Video angesprochen:

- *Angabe persönlicher Daten*
- *Herunterladen von Programmen*
- *Herunterladen von Musik*
- *Klingeltöne und Handylogos*
- *Suchmaschine Google*
- *Werbung im Internet*
- *Schutz vor Viren*
- *Werbung in E-Mails*
- *Schlechte oder böse Seiten*

Online-Shopping

Arbeitsblatt 1 (Seite 1)

Fragen und Tipps für groß und KLEIN

1. ***Ich finde auf einer Schülerseite ein schönes Gewinnspiel. Um mitmachen zu dürfen, soll ich aber meinen Namen und die Adresse angeben. Sollte ich das tun?***

   Auf keinen Fall! Im Internet dürft ihr niemals eure persönlichen Daten bekannt geben. Persönlichen Daten sind z. B.: Name, Adresse, Geburtsdatum, eure Telefonnummer und E-Mail-Adresse. Denn wenn ihr sie im Internet bekannt gebt, könnte es sein, dass ihr von anderen belästigt werdet. Solche Daten werden oft auch an Firmen weitergegeben, die euch dann mit Werbe-Mails zuschütten.

   Tipp: Wenn ihr ein tolles Gewinnspiel auf einer Kinderseite findet, sprecht mit euren Eltern! Die prüfen dann, ob das Gewinnspiel in Ordnung ist oder nicht und erst dann könnt ihr gemeinsam mit ihnen alles ausfüllen.

2. ***Kann es gefährlich werden, wenn ich mir ein Programm aus dem Internet herunterlade?***

   Dabei solltet ihr auf jeden Fall vorsichtig sein. Es gibt zwar gute kostenlose Programme, aber es werden auch viele angeboten, bei denen versteckte Kosten anfallen oder die Schaden auf eurem Computer anrichten können.

   Tipp: Ihr solltet nur mit euren Eltern zusammen etwas aus dem Internet herunterladen. Prüft gemeinsam, ob das gewünschte Programm überhaupt sinnvoll ist. Denn manchmal habt ihr bereits ein ähnliches Programm auf eurem Computer.

3. ***Meine Freunde laden sich oft Musik aus dem Netz. Ist das denn erlaubt?***

   Musik darf man nur von Seiten herunterladen, die eine Erlaubnis dafür geben, wenn nicht, ist dies verboten und kann bestraft werden.

   Tipp: Es gibt im Internet viele Seiten, bei denen es erlaubt ist Musik herunterzuladen. Allerdings muss man in der Regel etwas dafür bezahlen. Sucht mit euren Eltern Seiten aus, von denen die Musik kostenlos oder für wenig Geld heruntergeladen werden kann.

Arbeitsblatt 1 (Seite 2)

4. Ist ein Klingelton oder ein Handylogo immer kostenlos?

Nein, oder nur sehr selten. Das Bestellen von Klingeltönen, Logos und Handyspielen kostet fast immer Geld. Selbst hinter der Werbung „Die neusten Klingeltöne, jetzt kostenlos!" steckt oft eine Kostenfalle. Statt nur eines kostenlosen Klingeltons wird euch ein ganzes Abo angedreht. Dann müsst ihr alle Nasen lang für neue Klingeltöne zahlen, ob ihr sie wollt oder nicht. Um euch zu täuschen, wird auch manchmal nur der Preis für eine Handyminute angegeben. Dass das Herunterladen des Klingeltons viele Minuten dauert, wird nicht gesagt. Seid ihr auf ein Abonnement reingefallen? Dann lasst es von euren Eltern sofort kündigen.

Tipp: Es gibt Seiten, wo ihr euch kostenlos eigene Klingeltöne mixen könnt. Zum Beispiel: www.checked4you.de. Klickt auf die Rubrik „Handy + Telefon" und dann auf „Extras".

5. Darf ich auch bei Google suchen, wenn meine Kindersuchmaschine nichts gefunden hat?

Sucht bei großen Suchmaschinen wie Google bitte nur zusammen mit euren Eltern oder Lehrern! Diese Suchmaschinen sind für die Erwachsenen. Sie liefern oft Millionen Treffer. Deshalb ist es sehr schwer für euch, sich dort zurechtzufinden. Wenn ihr dort etwas suchen wollt, lasst euch von den Großen helfen.

Tipp: Überlegt euch, was ihr zu einem Thema wissen wollt. Je genauer ihr fragt, desto größer ist die Chance, dass die besten Treffer ganz oben stehen

6. Was mache ich mit der vielen Werbung, die auf manchen Seiten auftaucht?

Im Internet gibt es auf vielen Seiten bunt blinkende Werbung. Solche Werbebanner niemals anklicken. Egal was sie euch versprechen! Manchmal legt sich die Werbung sogar über den Text, den ihr gerade lesen wolltet. Es gibt auch Firmen, die locken euch mit Spielen, wenn ihr dann auf die Werbung klickt, werdet ihr nur zu noch mehr Werbung oder Verkaufsangeboten geführt.

Tipp: Wenn sich ständig solche Werbeseiten öffnen, ohne dass ihr das wollt, dann schaltet am besten den Computer ganz aus und startet ihn neu.

Arbeitsblatt 1 (Seite 3)

7. Wie kann ich meinen Computer vor Viren schützen?

Viren kann man vor allem durch E-Mails oder beim Herunterladen von Dateien aus dem Internet bekommen. Deswegen öffnet niemals den Anhang einer E-Mail, wenn euch der Absender unbekannt ist.

Zum Schutz muss auf eurem Computer ein Anti-Viren-Programm installiert werden. Denn Viren können auf eurem Computer großen Schaden anrichten oder ihn sogar zerstören. Bittet deshalb eure Eltern, das Anti-Viren-Programm regelmäßig zu aktualisieren.

Tipp: Löscht E-Mails, wenn ihr nicht wisst, von wem sie sind. Und öffnet auch nicht die Anhänge! Sogar in Text- oder Bilddateien können Viren stecken.

8. An meine E-Mail-Adresse wird ständig lästige Werbung geschickt. Was kann ich dagegen tun?

Dagegen gibt es einen guten Trick: zwei E-Mail-Adressen! Eine E-Mail-Adresse nur für gute Freunde und eine zweite für die allgemeine Internetnutzung.

Lästige Werbe-E-Mails werden „Spam“ (gesprochen: „Späm“) genannt, mit denen man euch irgendwelche Dinge anbietet und die euer Postfach verstopfen. Manchmal können sie sogar Viren enthalten. Deshalb dürft ihr auf solche E-Mails niemals antworten. Auch nicht, um euch zu beschweren. Denn dann weiß der Absender, dass es eure Adresse tatsächlich gibt und schickt euch noch mehr Werbe-Mails.

Tipp: Die erste E-Mail-Adresse solltet ihr wirklich nur für Freunde verwenden. Die zweite könnt ihr z. B. für die Anmeldung im Chat und so weiter benutzen. Dieses Postfach lasst jedoch bitte regelmäßig von euren Eltern prüfen. Sie können dabei gleich alle lästigen Mails löschen. Bei zu viel Werbung sollten euch die Eltern am besten eine neue E-Mail einrichten.

9. Was soll ich machen, wenn ich aus Versehen auf eine schlechte oder böse Seite geraten bin?

Wenn euch so etwas passiert, sagt euren Eltern Bescheid. Und keine Angst: Nicht ihr seid schuld, wenn ihr auf solche Seiten kommt, sondern die Menschen, die diese Seiten ins Netz gestellt haben.

Tipp: Es gibt eine Stelle, wo ihr euch gemeinsam mit euren Eltern über schmutzige oder böse Internetseiten beschweren könnt. Die Menschen dort kümmern sich dann um solche Seiten.

Die Adresse lautet: **www.jugendschutz.net** – Zentralstelle für Jugendschutz im Internet
E-Mail: **hotline@jugendschutz.net**
Beschwerdeformular: **www.jugendschutz.net/hotline**

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Soziale Netzwerke

studiVZ, facebook & Co

Was sind soziale Netzwerke?

In sozialen Netzwerken (englisch: „Social Communities“ oder „Social Networks“) und im Internet habt ihr die Möglichkeit, eigene Inhalte in Form von Texten und Bildern zu veröffentlichen, euch mit anderen zu vernetzen und im Gegenzug auf Veröffentlichungen der anderen, mit Kommentaren zu reagieren. Des Weiteren könnt ihr Freundeslisten anlegen und mit anderen Informationen austauschen.

Über verschiedene Kommunikationswege (z. B. Chats, Foren) im Internet hat jeder die Möglichkeit, mit anderen Menschen in Kontakt zu treten. Gerade die Preisgabe von persönlichen Daten in sozialen Netzwerken birgt auch Risiken und Gefahren.

Welche Gefahren können mir in sozialen Netzwerken begegnen?

Es gibt verschiedene Gefahren in sozialen Netzwerken.

Offenlegung persönlicher Daten

Die Preisgabe von persönlichen Daten (E-Mail-Adressen, Telefonnummern, etc.) kann von Firmen missbräuchlich genutzt werden, um euch mit Werbung zu bombardieren. Dafür solltet ihr in euren Privatsphäre-Einstellungen, in eurem Account die Einstellungen so vornehmen, dass nicht alle von euch eingestellten Daten auch für alle sichtbar sind. Ebenfalls ist darauf zu achten, dass potentielle Arbeitgeber in den sozialen Netzwerken nach Informationen ihrer Bewerber suchen. Freizügige Fotos können dabei ein Ausschlusskriterium sein. Einmal eingestellte Daten können von Dritten auf deren Computer archiviert werden und so auf anderen Seiten im Internet verwendet werden.

Phishing

Über gefälschte Webseiten versuchen Betrüger an die Zugangsdaten für soziale Netzwerke heranzukommen. Über Links in einer gefälschten E-Mail könnt ihr auf eine Seite gelangen, die der des sozialen Netzwerks täuschend ähnlich sieht. Versucht ihr euch dort einzuloggen, können die Betrüger Nutzername und Passwort abfischen und haben ab dann vollen Zugriff auf den Account, können Daten einsehen und ändern, Nachrichten verschicken und chatten. Eure Freunde merken davon nichts und denken alle Änderungen und Nachrichten kämen von euch.

Identitätsdiebstahl

Kriminelle versuchen zunehmend, bestehende Nutzer-Accounts zu hacken, um diese Identität für ihre Betrügereien zu nutzen. Oftmals täuschen diese Hacker nach Übernahme eines Accounts eine Notsituation vor und bitten die vernetzen Freunde um finanzielle Hilfe. Das über das Nutzerprofil erlesene Wissen kann dazu beitragen, das Vertrauen zu untermauern und Freunde zu täuschen.

„Unechte“ Profile werden zunehmend dazu genutzt, Personen zu schaden. Diebe können so zum Beispiel ausspionieren, wann jemand im Urlaub ist und die Wohnung leer steht.

Mobbing

Mobbing, das Schikanieren von anderen Personen, um sie auszugrenzen, ist in sozialen Netzwerken weit verbreitet. Freundschaften sind in sozialen Netzwerken schneller geschlossen als in der „realen“ Welt. So gelangen Informationen an Personen, die diesen sonst vielleicht nicht anvertraut worden wären. Wer böswillige Absichten hat, kann diese Informationen dafür nutzen, um jemanden bewusst bloßzustellen oder ihn böse zu beschimpfen. Oft legen sich fremde Personen „unechte“ Profile an, in denen sie sich als eine andere Person ausgeben. So können sie euch über das soziale Netzwerk belästigen.

Soziale Netzwerke

Verbreitung von Schadsoftware

Das Vertrauen der Nutzer in die sozialen Netzwerke ist meist groß. Betrüger haben deshalb eine gewohnte Masche auf diese Plattformen übertragen: Sie verschicken Nachrichten, die einen Link auf manipulierte Webseiten enthalten. Über diese Seiten werden dann die Schadprogramme (z. B. Viren oder Trojaner) verbreitet. Manche soziale Netzwerke bieten Zusatzanwendungen (z. B. Minispiele) an, die ihr eurem Profil hinzufügen könnt. Problematisch ist, dass diese Anwendungen von Drittanbietern stammen, deren Sicherheitsstandards nicht zwangsläufig denen der sozialen Netzwerke entsprechen müssen.

Was kann ich für einen sicheren Umgang mit sozialen Netzwerken tun?

- Gebt so wenig persönliche Informationen wie möglich in eurem Profil an!
- Lest die allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des von euch genutzten sozialen Netzwerks!
- Nehmt nicht jede Freundschaftsanfrage an, sondern schaut euch die Person erst an, ob ihr sie kennt, wenn nicht, dann lasst lieber die Finger davon!
- Wenn ihr von fremden Personen dauerhaft belästigt werdet, dann meldet diese Nutzer auf der Plattform und sprecht darüber auch mit vertrauten Personen!
- Verwendet für jede Internetanwendung, insbesondere auch wenn ihr in verschiedenen sozialen Netzwerken angemeldet seid, ein unterschiedliches und sicheres Passwort!
- Gebt keine vertraulichen Informationen über euren Arbeitgeber und eure Arbeit preis!
- Achtet genau darauf, welche Fotos ihr von euch preisgeben wollt! Partyfotos und andere Schnappschüsse könnten euch in Schwierigkeiten bringen!
- Wenn ihr „zweifelhafte" Anfragen von euch bekannten Personen erhaltet, erkundigt euch außerhalb sozialer Netzwerke in einem persönlichen Gespräch, was die andere Person damit bezweckte!
- Klickt nicht wahllos auf Links – soziale Netzwerke werden verstärkt von Betrügern genutzt, um eure Daten zu stehlen!
- Wenn euch beim Surfen in sozialen Netzwerken etwas komisch vorkommt, dann sprecht mit euren Eltern oder mit Freunden darüber und überlegt gemeinsam, wie ihr weiter vorgeht!

Soziale Netzwerke – Unterrichtseinheit

Schwerpunkt: Soziale Netzwerke und Cybermobbing

Zielgruppe: ab Klasse 7

Dauer: 3 – 6 Zeitstunden

Lernziele:

- Die Schülerinnen und Schüler reflektieren ihre eigene Medienausstattung und Mediennutzung und setzen sich mit den Meinungen der Mitschüler zum Medienumgang auseinander.

- Die Schülerinnen und Schüler nehmen kritisch Stellung zu möglichen Inhalten von Profilen aus sozialen Netzwerken.

- Die Schülerinnen und Schüler beschäftigen sich mit der Problematik des Cybermobbings. Sie wissen was Cybermobbing ist. Sie lernen welche Ursachen und Folgen Cybermobbing haben kann. Es werden ihnen mögliche Gefahren aufgezeigt und zusammen nach Problemlösungen gesucht.

Materialien:

Flipchart, Stifte, AB 1 Meinungen zum Medienumgang, AB 2 Kartenabfrage, AB 3 Profilbeispiele, Musikvideo „Ich bin online :(", Simple Show „Soziale Netzwerke", PCs mit Internetzugang ohne Zugangsbeschränkung

Methoden:

Einzelarbeit, Partnerarbeit, Gruppenarbeit, Gesprächskreis, Diskussionen

Unterrichtsplanung:

Als Einstieg in das Thema Internet und soziale Netzwerke schreiben die Schülerinnen und Schüler ihre Medienausstattung und -nutzung und hier besonders die Nutzung des Internets auf. Dafür wird an einem Flipchart eine Tabelle aufgezeichnet (AB 1). Diese Aufgabe kann als Gruppenarbeit erledigt werden und wird anschließend der Klasse vorgestellt. Wichtig ist dabei, dass sich die Schülerinnen und Schülern auf Medien beziehen sollen, die sie in ihrem Zimmer zur Verfügung haben. Es ist ratsam, dass sich die Lehrkraft im Vorfeld mit den Unterschieden zwischen Instant Messengern, Chats und sozialen Netzwerken beschäftigt.

Als Einstieg in die Thematik eignet sich ebenfalls die Simple Show „Soziale Netzwerke", weil hier ein guter Überblick gegeben wird, was soziale Netzwerke sind und welche Risiken auftreten können.

Um die vorherrschende Meinung zum Thema in der Klasse noch deutlicher werden zu lassen, bekommt jeder der Schülerinnen und Schüler einen Stapel mit kleinen Kärtchen, auf denen verschiedene Aussagen stehen (AB 2). Die Schülerinnen und Schüler haben die Aufgabe diese Aussagen zu lesen und sich zu entscheiden, ob sie der Aussage eher zustimmend oder ablehnend gegenüber stehen. Es sollen zwei Stapel gebildet werden. Wenn alle die Karten für sich geordnet haben, werden diese auf den Boden gelegt. In der Mitte hat die Lehrkraft die Zettel mit den Buchstaben in einer anderen Farbe untereinander ausgelegt. Links und rechts daneben wird jeweils ein lachender und ein weinender Smily ausgelegt. Nun ordnen die Schülerinnen und Schüler ihre Karten den Smilys zu. Die A-Zustimmungskärtchen in eine Reihe, darunter die B-Zustimmungskärtchen usw. Das Gleiche auch für die Meinungen denen sie nicht zugestimmt haben. Über die entstandenen Balkendiagramme kann diskutiert werden. Welche Meinungen wurden überwiegend abgelehnt und welchen wurde überwiegend zugestimmt? Welche Gründe geben die Schülerinnen und Schüler für ihre Entscheidung an?

Soziale Netzwerke – Unterrichtseinheit

Daran schließt sich der nächste Block an, in dem die Schülerinnen und Schüler verschiedene Profilbeispiele betrachten. Hier empfiehlt sich eine Partnerarbeit. Sie erhalten die Beispielprofile aus dem Arbeitsmaterial Nr. 3 (AB 3) welches sie unter kritischen Gesichtspunkten bearbeiten.

Im nächsten Schritt beschäftigen sich die Schülerinnen und Schüler mit dem Thema Cybermobbing. Zuallererst geht es darum, eine gemeinsame Definition zu finden. Hierbei gibt es zwei Möglichkeiten. Entweder die Schülerinnen und Schüler erarbeiten sich selbstständig Fakten, die mit dem Mobbing im Zusammenhang stehen. Diese werden an der Tafel gesammelt, um dann daraus eine Definition abzuleiten. Die zweite Variante ist, die Schülerinnen und Schüler im Internet nach geeigneten Definitionen von Cybermobbing suchen zu lassen. Anschließend tragen sie ebenfalls ihre Ergebnisse vor und arbeiten dann an einer eigenen Definition.

Das Musikvideo „Ich bin online :(“ dient als Impulsgeber, um noch tiefer in die Thematik einzusteigen. Die Schülerinnen und Schüler schauen das Video und im Anschluss wird über das Gesehene gesprochen. Hierbei werden von der Lehrkraft Fragen zur Täter- und Mitläuferschaft gestellt, d. h.: Was bewegt jemanden, andere zu mobben bzw. dort mitzumachen? Welche Folgen hat eine Mobbingattacke für das Opfer?

Zum Abschluss des Themas steht die Frage: Was können wir gegen Cybermobbing an unserer Schule tun? Dazu sollen die Schülerinnen und Schüler in Gruppenarbeit verschiedene Ideen sammeln. Anschließend werden diese im Plenum vorgestellt. Aus den zusammengetragenen Punkten wird eine Liste mit den wichtigsten Maßnahmen erstellt (nicht mehr als zehn). Diese kann für weitere Klassen vervielfältigt werden.

Hausaufgabenvorschlag:

Die Schülerinnen und Schüler recherchieren auf der Internetseite www.bsi-fuer-buerger.de nach

Tipps zur sicheren Nutzung von sozialen Netzwerken.

Mit den angegebenen Tipps gestalten die Schüler einen kleinen Flyer.

Soziale Netzwerke

Arbeitsblatt 1

Die Schülerinnen und Schüler haben die Aufgabe, in einer Gruppenarbeit diese Tabelle zu ihrer Medienausstattung und Mediennutzung auszufüllen. In der Spalte „Medien" sollen diejenigen Medien stehen, die die Schülerinnen und Schüler in ihrem Zimmer haben. Die weiteren Stichworte richten sich an die Nutzung des Internets.

Mögliche Fragen der Lehrkraft:

- Wo wird recherchiert, wenn ich zu einem Thema etwas wissen möchte? (z. B. Suchmaschinen)
- Kaufe ich im Internet ein, wenn ja, wo und wer bezahlt das?
- Spiele ich online verschiedene Spiele, wenn ja, wo?
- In welchen Sozialen Netzwerken bin ich angemeldet?

Name	Medien	Recherche	Shopping	Games	Soziale Netzwerke

Soziale Netzwerke

Arbeitsblatt 2

Meinungskärtchen für die Gruppendiskussion

Diese Kärtchen vervielfältigen und ausschneiden.

Es sollte für Jugendliche eine gesetzlich festgesetzte Nutzungsdauer von 5 Stunden in der Woche für das Internet geben. A	Jugendliche sind nur in sozialen Netzwerken angemeldet, um andere auszuspionieren. D
Bilder von Partys ins Netz zu stellen, finde ich geschmacklos. B	Mobbingattacken im Internet sind nicht so schlimm, wie alle immer sagen. E
Ich weiß genau über die Gefahren im Internet Bescheid. C	Man sollte sich so früh wie möglich mit dem Computer und dem Internet auseinandersetzen, das ist gut für das spätere Leben. F

Soziale Netzwerke

Arbeitsblatt 3

Die Schülerinnen und Schüler sollen sich kritisch mit den Inhalten dieser Profile auseinandersetzen.

Mögliche Fragen:

- Welche Inhalte sind harmlos?
- Welche dargestellten Inhalte sind kritisch zu sehen und warum?
- Was ist auf dem Foto zu sehen?
- Was ist auffällig an der Gruppenzugehörigkeit?

Netzwerk-VZ

Suche Kontext Handy Einladen Hilfe Blog Raus hier

Bela Müllers Seite

Belas Fotoalben
Belas Freunde
Bela eine Nachricht schicken
Bela zuwinken
Bela melden/ignorieren

Fotoalben

Gemeinsame Freunde

Freunde

SV Klein Werder

Checker

Informationen

Name:	Bela Müller
Geschlecht:	männlich
Geburtstag:	16.09.1999
Schule:	Gustav-Adolf- Sekundarschule
Auf der Suche nach:	Spaß und netten Leuten
Beziehungsstatus:	single
Politische Einstellung:	egal
Interessen:	Party machen, Faulenzen
Musik:	alles was rockt
Lieblingsfilm:	och da gibt es viele
Lieblingsfach:	Sport, Geografie
Hassfach:	Mathe, Deutsch, Englisch
Über sich selbst:	Kommt und fragt mich, aber sonst ich bin für alles zu haben....

Kontakt

Icq:	456209336
skype:	bela99
E-Mail:	kingbela@network.com
Mobil:	01522/508033344

Gruppen

- Ich hasse Schule! Du auch?
- Beim Streit gibt es immer 2 Standpunkte, meinen und den falschen!
- Wir lieben Lebensmittel, besonders flüssig und hochprozentig!!!
- Steckdosen sind gefährlich, ein gutes Beispiel ist Bollo
- Wir hassen Frau Walter!
- Scheiß Borussia, die wahren Helden sind die Bayern
- Blau ist keine Farbe, sondern ein Zustand

Netzwerk-VZ

Suche Kontext Handy Einladen Hilfe Blog Raus hier

Checkers Seite

SV Klein Werder

Checkers Fotoalben
Checkers Freunde
Checker eine Nachricht schicken
Checker zuwinken
Checker melden/ignorieren

Fotoalben

Gemeinsame Freunde

Freunde

Bela Müller

Informationen

Name:	Checker
Geschlecht:	männlich
Geburtstag:	10.02.2000
Schule:	Hauptschule Eichdamm
Auf der Suche nach:	dem Sinn des Lebens
Beziehungsstatus:	verliebt
Politische Einstellung:	???
Interessen:	Liebe, Sex und Zärtlichkeit
Musik:	Charts
Lieblingsfilm:	Batman
Lieblingsfach:	hab ich nicht
Hassfach:	alle
Über sich selbst:	ich stelle keine blöden Fragen, ich bin cool Alter

Kontakt

skype:	checker2000
E-Mail:	Checkdat@work.com

Gruppen

- Schick mir n Kettenbrief & ich sorg persönlich für deinen Untergang
- Beim Streit gibt es immer 2 Standpunkte, meinen und den falschen!
- Schule?? Ich denke Kinderarbeit ist verboten?
- Steckdosen sind gefährlich, ein gutes Beispiel ist Bollo
- Eine Party ohne Alk, wie geht das denn?
- Fußball-Liebhaber
- Bettina ist eine Schlampe! Wer das auch denkt, kommt hier rein...
- Wir wollen den Rekord von 15 000 Mitglieder brechen...
- Batman - forever!!!
- Die am 10.02. Geburtstaghaber!

Netzwerk-VZ

Suche Kontext Handy Einladen Hilfe Blog Raus hier

Lena B.s Seite

Lena B.s Fotoalben
Lena B.s Freunde
Lena B. Eine Nachricht schicken
Lena B. zuwinken
Lena B. Melden/ignorieren

Fotoalben

Lena B. hat keine Fotoalben

Gemeinsame Freunde

Du hast keine gemeinsamen Freunde

Freunde

Du kannst Lena B.s Freunde nicht sehen

Informationen

Name:	Lena B.
Geschlecht:	weiblich
Geburtstag:	30.01.1996
Schule:	Berg-Gymnasium
Auf der Suche nach:	interessanten Menschen
Beziehungsstatus:	verliebt
Politische Einstellung:	grün
Interessen:	Lesen, Freunde treffen
Musik:	Rhianna
Lieblingsfach:	ich mag eigentlich alles

Kontakt

icq:	878787879

Gruppen

Lena B. ist noch in keiner Gruppe

Pinnwand

Trixxy schrieb

Hallo Süße! Ich lass ein paar liebe Grüße auf deiner Pinnwand! Knutsch

Netzwerk-VZ

Suche | Kontext | Handy | Einladen | Hilfe | Blog | Raus hier

Sweet Sisters Seite

Sweet Sisters Fotoalben
Sweet Sisters Freunde
Sweet Sister eine Nachricht schicken
Sweet Sister zuwinken
Sweet Sister melden/ignorieren

Fotoalben

Gemeinsame Freunde

Du hast keine gemeinsamen Freunde

Freunde

Peter S.

Lutz Blume

Informationen

Name:	Sweet Sister
Geschlecht:	weiblich
Geburtstag:	18.06.1989
Schule:	Realschule Willdensleben
Auf der Suche nach:	süßen Jungs
Beziehungsstatus:	verzaubert
Politische Einstellung:	weiß nicht
Interessen:	Musik, Tanzen, Shoppen
Musik:	alles was so richtig fetzt
Lieblingsfilm:	keine
Lieblingsfach:	Kunst, Musik, Sport
Hassfach:	Mathe, Englisch
Über sich selbst:	man findet mich meistens im “Netz-Café”

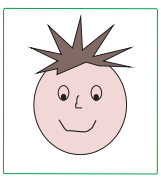
Kontakt

icq:	999995555
E-Mail:	sweetpussycat@net.de

Gruppen

- Hier kommen nur coole Mädchen rein...
- ~Ich bewerfe dich solang mit Wattebällchen bis du blutest~
- Abschreiben?! Wir nennen das Teamwork!

Pinnwand



Lutz Blume schrieb

Seit der Party letzten Samstag muss ich immer an dich denken... Du geile Pussy!!!
Ruf mich an, wenn du Lust hast:
0199/71234837

Online-Banking

Online-Banking – was ist das?

Mit Online-Banking wird die Abwicklung von Bankgeschäften über das Internet bezeichnet. Die Angebotspalette reicht vom bloßen Abfragen des Kontostands oder einzelner Umsätze über die Durchführung von Überweisungen und die Einrichtung von Daueraufträgen bis hin zu individuellen Auswertungen der Kontobewegungen.

Online-Banking ist für viele Menschen heute ganz selbstverständlich. Jedoch gilt auch beim Online-Banking zu beachten, dass Kriminelle versuchen, Konto- und Kreditkartendaten der Nutzer auszuspähen (Phishing) und mit ihrer Hilfe an das Geld der Bankkunden zu kommen.

Wie funktioniert Online-Banking?

Online-Banking wird über das Internet angeboten. Die von den Banken verwendeten Verbindungen werden heute üblicherweise über SSL (Secure Sockets Layer) verschlüsselt angeboten. Dies erkennt ihr daran, dass die URL mit „https“ statt „http“ beginnt.

Der Zugang zum persönlichen Konto erfolgt zumeist über das PIN/TAN-System. Dabei gibt der Benutzer neben seiner Kontonummer eine persönliche Identifikationsnummer (PIN) ein. Jede Aktion kann jedoch erst getätigt werden, wenn eine Transaktionsnummer (TAN) eingegenben wird, die jeweils nur einmal gültig ist.

Verschiedene Verfahren:

iTAN

Die TANs auf der Liste sind durchnummeriert (indiziert). Wenn eine Transaktion erfolgt ist, wird eine bestimmte TAN (z. B. Nr. 31) auf eurer Liste abgefordert, diese ist an den aktuellen Auftrag gebunden und kann nicht beliebig verwendet werden.

mTAN oder SMSTAN

Hierbei habt ihr keine seperate TAN-Liste in den Händen, sondern es wird bei jeder Transaktion eine sogenannte „mobile TAN“ als SMS auf eurer Handy geschickt. Diese TANs haben eine zeitlich begrenzte Gültigkeit, d. h. sie müssen umgehend benutzt werden. Der Nachteil bei diesem Verfahren ist, dass zusätzliche Kosten für die Übertragung der TAN per SMS auf euch zu kommen können.

chipTAN-Verfahren

Bei diesem Verfahren erhaltet ihr von eurer Bank einen TAN-Generator mit Ziffernfeld und Karteneinschub, auf dessen Rückseite zusätzlich fünf optische Sensoren angebracht sind. Nach Eingabe einer Transaktion – etwa einer Überweisung – erscheint auf dem PC-Bildschirm eine Grafik mit fünf flackernden schwarzweißen Flächen. Ihr müsst nun eure Bankkarte in den Generator stecken und diesen an die Grafik auf dem Monitor halten. Von dort aus werden Informationen als Lichtsignale an den Generator übertragen, der in seinem Display danach die Kontonummer des Empfängers und den Überweisungsbetrag anzeigt. Nachdem ihr diese bestätigt habt, errechnet der Generator eine TAN.

Sicherheitstipps für das Online-Banking

- Achtet darauf, dass die Datenübertragung bei WLAN-Verbindungen ausreichend verschlüsselt ist!
- Eure Daten müssen immer verschlüsselt übertragen werden! Das erkennt ihr am „https“ in der Internetadresse. Oft erscheinen auch ein Sicherheitsschloss oder ein Schlüssel als Symbol in der Statusleiste.
- Wählt für euer Passwort eine schwer zu erratende Buchstaben-/Zahlenkombinationen, schützt diese Zugangsdaten vor Dritten und speichert diese niemals ab!
- Wenn ihr Online-Banking betreibt, dann möglichst nur von eurem eigenen Rechner!

Online-Banking

- Achtet darauf, keine Software aus unseriösen oder unsicheren Quellen auf eurem Computer zu speichern!
- Schützt euern PC vor unerlaubten Zugriffen!
- Benutzt immer eine aktuelle Virenschutzsoftware und aktiviert eure Firewall!
- Spielt aktuelle Sicherheitsupdates für das Betriebssystem ein!
- Überprüft regelmäßig eure Kontoauszüge und wendet euch bei Auffälligkeiten sofort an eure Bank!
- Vereinbart mit eurer Bank ein Limit für tägliche Geldbewegungen beim Online-Banking!
- Seid vorsichtig, wenn ihr E-Mails erhaltet, in denen ihr aufgefordert werdet, eure Kontodaten zu aktualisieren! Betrüger können auf diese Weise versuchen, euch auf gefälschte Seiten von eurer Bank zu locken, um euch persönliche Informationen zu entlocken.
- Sperrt sofort euren Online-Bankingzugang, wenn euch etwas verdächtig vorkommt!

Was tun, wenn doch etwas passiert ist?

Wenn ihr den Eindruck oder den Verdacht habt, dass etwas nicht stimmt, solltet ihr sofort aktiv werden:

- Sperrt unverzüglich euer Bankkonto und den Zugang zum Online-Banking! Am schnellsten geht das, indem ihr zum Beispiel die Anmeldemaske zum Online-Banking aufruft und dreimal hintereinander die falsche PIN eingebt. Oder ihr ruft den zentralen Sperr-Notruf 116 116 (aus dem Ausland +49 116 116) an und lasst euch euern Zugang telefonisch sperren.
- Danach wendet euch an eure Bank und meldet die Auffälligkeiten! Gegebenenfalls besteht die Möglichkeit, Kontobewegungen rückgängig zu machen.
- Prüft umgehend die Kontoumsätze anhand des Papierauszuges!
- Solltet ihr tatsächlich Opfer eines Phishingangriffs mittels eines Trojaners geworden sein, müsst ihr euren PC fachgerecht von der Schadsoftware befreien lassen!
- Erstattet Anzeige bei der Polizei!

Quelle:

CD-ROM „Ins Internet – mit Sicherheit“ – Bundesamt für Sicherheit in der Informationstechnik/
www.bsi-fuer-buerger.de

Online-Banking I – Unterrichtseinheit

Schwerpunkt: Sicherheit

Zielgruppe: ab Klasse 10

Dauer: 1 Zeitstunde

Lernziele:

- Die Schülerinnen und Schüler lernen verschiedene Möglichkeiten des elektronischen Zahlungsverkehrs kennen, können die Gefahren hierbei abschätzen.
- Die Schülerinnen und Schüler schulen ihre Fähigkeiten, sich selbstständig anhand von Arbeitsmaterialien Informationen einzuholen und hieraus die wichtigsten Punkte zu filtern.
- Die Schülerinnen und Schüler kennen die Struktur von Online-Banking-Systemen und wissen, wie wichtig es ist, konzentriert zu arbeiten.
- Die Schülerinnen und Schüler kennen die Gefahren, die Online-Banking mit sich bringt.

Materialien:

Tafel, DVD-Player, Fernseher, internetfähige PCs ohne Zugangsbeschränkung (Computerkabinett), farbige Stifte, AB 1 „Online-Banking I", AB 2 „Online-Banking II", Simple Show „Online-Banking",

Methoden:

Einzelarbeit, Gruppenarbeit, Gesprächskreis, Diskussionen, Recherche

Unterrichtsplanung:

Zu Beginn der Einheit schauen sich Schüler und Lehrer gemeinsam die Simpleshow „Online-Banking" an. Im Anschluss daran werden im Plenum Gelegenheiten gesammelt, bei denen die Schüler schon einmal mit Online-Banking in Berührung gekommen sind. Im Gespräch wird diskutiert, welche Erfahrungen die Schüler damit machten, welche Alternativen es eventuell gab und inwieweit sie diesen Dienst nutzen.

Im Anschluss an die Diskussion sollen Gründe für und gegen Online-Banking gesammelt und an der Tafel festgehalten werden.

Gründe für Online-Banking:

- *Bank hat immer geöffnet*
- *man ist nicht auf das Filialnetz der Banken angewiesen*
- *meist kostengünstiger als Überweisung in der Filiale*
- *auch andere Dienste wie Daueraufträge oder Kontoauszüge nutzbar*
- *Überweisungen können sofort (nach einem Kauf) getätigt werden*

Gründe gegen Online-Banking:

- *Gefahr von Phishing*
- *man muss sich viele Zahlen und Passwörter merken, die man sicher verwahren muss*
- *Barzahlung lässt immer weniger Rückschlüsse zu, weil sie nicht auf dem Kontoauszug erscheint und Banken nicht nachvollziehen können, wofür genau der Kunde Geld ausgibt*
- *sehr umständlich und für ältere Menschen nicht immer verständlich*

Nachdem die Vor- und Nachteile gemeinsam diskutiert wurden, wird das Arbeitsblatt 1 bearbeitet.

Arbeitsblatt 1

Das Arbeitsblatt kann als kleiner Test von der Lehrkraft oder innerhalb der Unterrichtsstunde gemeinsam ausgewertet werden. Eventuelle Fragen der Schüler werden beantwortet.

Zum Schluss der Unterrichtsstunde wird die Demokonto-Funktion der Postbank genutzt. Hierzu nutzen die Schüler das Arbeitsblatt 2.

Arbeitsblatt 2

Hausaufgabenvorschlag:

Die Schüler recherchieren auf der Internetseite www.bsi-fuer-buerger.de welche TAN-Verfahren es gibt.

Online-Banking II – Unterrichtseinheit

Schwerpunkt: Sicherheit

Zielgruppe: ab Klasse 10

Dauer: 2 Zeitstunden

Lernziele:

- Die Schülerinnen und Schüler kennen die Gefahren, die Online-Banking mit sich bringt und wissen, wie sie sich schützen können.
- Die Schülerinnen und Schüler können das erlangte Wissen zusammenfassen und für andere kreativ aufbereiten.

Materialien:

farbige Stifte, farbiges Papier (A3 und A4), internetfähige PCs ohne Zugangsbeschränkung (Computerkabinett)

Methoden:

Einzelarbeit, Gruppenarbeit, Gesprächskreis, Diskussionen, Recherche, Kreativarbeit

Unterrichtsplanung:

Zu Beginn der zweiten Einheit werden die Inhalte aus Einheit 1 wiederholt. Mögliche Fragen werden beantwortet. Danach wird beispielsweise auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik www.bsi-fuer-buerger.de sowie im Flyer „Phishing“ zu Gefahren und Sicherheitsregeln für Online-Banking recherchiert. Die recherchierten Sicherheitshinweise werden zusammen mit dem eigenen Wissen aufbereitet und in Form einer Wandzeitung zusammengefasst. Diese wird anschließend im Klassenraum für alle sichtbar aufgehängt.

Sicherheitshinweise:

- *Defender und Firewall verwenden*
- *Löschen von Cookies*
- *Leeren des Caches und des Verlaufs*
- *Seite der Bank nicht aus Lesezeichen aufrufen, sondern immer wieder neu in Adresszeile eingeben*
- *vor Bestätigen immer Daten genau prüfen*
- *TAN nur eingeben, wenn man sich auf https-Seite befindet*
- *TANs niemals auf Computer speichern*
- *sicheres Passwort (PIN) wählen*
- *Online-Banking-Limit festlegen*
- *Online-Banking sofort sperren, wenn etwas verdächtig vorkommt*

Online-Banking I

Arbeitsblatt 1

Timm hat sich von seinem Kollegen Jonas Geld geborgt. Die 50 Euro möchte er nun per Online-Banking an Jonas zurückgeben.

1. Welche Nummer/n muss Tim beim Online-Banking eingeben?

   □ nur PIN □ nur TAN □ beide

2. Timm ist bei der Sparkasse. Wann kann er online überweisen, wann hat seine Onlinebank geöffnet?

3. Was braucht Timm alles, um per Online-Banking überweisen zu können?

4. Manchmal erhält Timm auch ziemlich komische Mails von seiner Bank. Von seiner Freundin Melanie, die mal bei einer Bank gearbeitet hat, weiß er aber, dass es sich dabei um so genannte „Phishing-Mails" handelt. Welche Informationen versuchen die Gauner von Timm in diesen Mails zu erhalten?

5. Timm hat nun per Online-Banking die geborgten 50,- € an Jonas überwiesen. Abgebucht wurden aber 500,- €. Wie konnte das passieren?

Online-Banking I

Lösungen zu Arbeitsblatt 1

Timm hat sich von seinem Kollegen Jonas Geld geborgt. Die 50 Euro möchte er nun per Online-Banking an Jonas zurückgeben.

1. Welche Nummer/n muss Timm beim Online-Banking eingeben?

   □ nur PIN □ nur TAN □ beide

   (beide)

2. Timm ist bei der Sparkasse. Wann kann er online überweisen, wann hat seine Onlinebank geöffnet?

   (immer)

3. Was braucht Timm alles, um per Online-Banking überweisen zu können?

   (PC,

   Internet-Anschluss,

   Pins und Tans,

   Kontodaten des Empfängers,

   Girokonto muss für Online-Banking freigeschaltet sein)

4. Manchmal erhält Timm auch ziemlich komische Mails von seiner Bank. Von seiner Freundin Melanie, die mal bei einer Bank gearbeitet hat, weiß er aber, dass es sich dabei um so genannte „Phishing-Mails" handelt. Welche Informationen versuchen die Gauner von Timm in diesen Mails zu erhalten?

   (Bankverbindung, Namen, PIN und TANs)

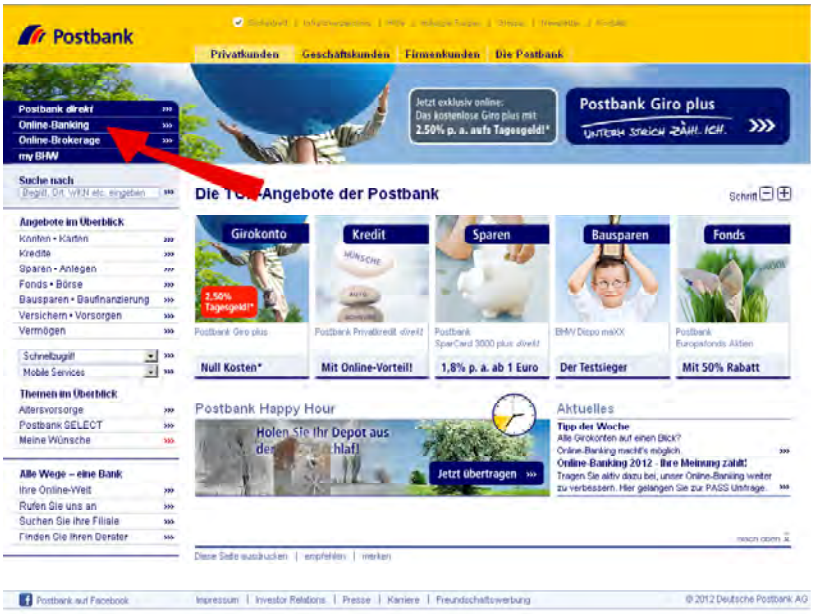
5. Timm hat nun per Online-Banking die geborgten 50,- € an Jonas überwiesen. Abgebucht wurden aber 500,- €. Wie konnte das passieren?

   (falschen Betrag eingegeben – deshalb immer aufpassen)

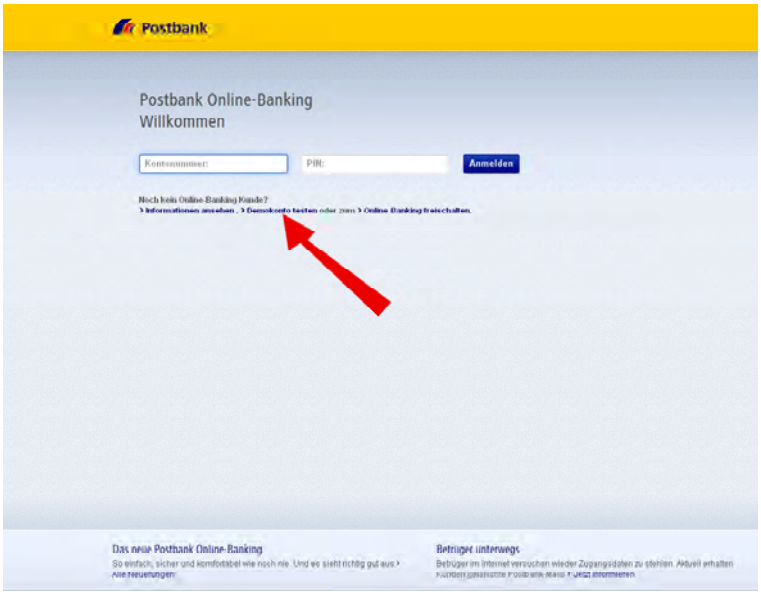
Online-Banking II

Arbeitsblatt 2

Auch Timms Chefin nutzt Online-Banking und überweist Timms Gehalt bequem über das Internet. Vollziehe nach, wie Frau Pfiffig dabei vorgeht. Gehe dazu auf die Seite www.postbank.de und wähle hier den Reiter Online-Banking.

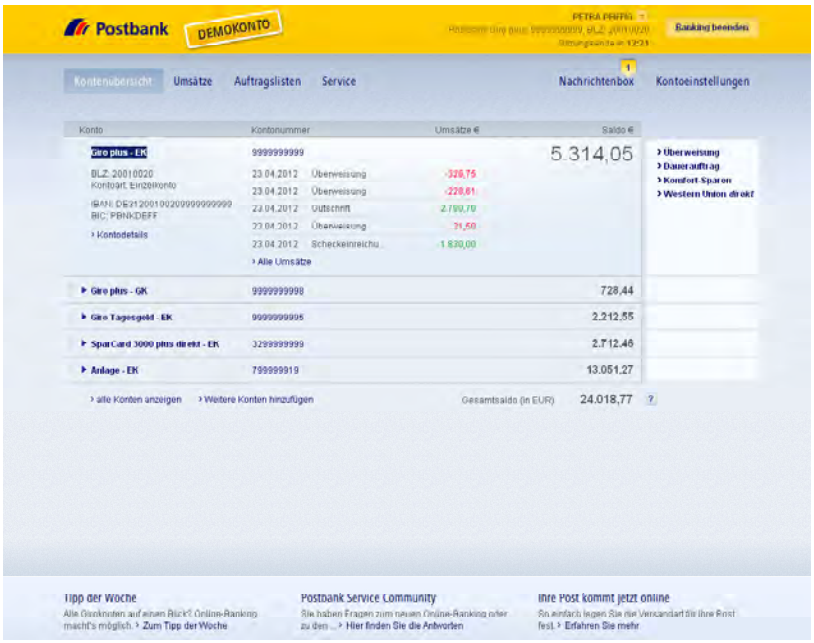


Klicke hier auf den Button Demokonto testen...



Online-Banking II

... und wähle das Giro plus – EK. Überprüfe, ob du dich auf einer sicheren Seite befindest.
Woran kannst du das erkennen?



Überweise nun Timms Gehalt von 1000,00 Euro auf folgendes Konto:

Empfänger: Timm Schmidt

Konto-Nr: 987 654 321

BLZ: 810 532 72

Verwendungszweck: Überlege dir einen!

Lass dir nun eine TAN per SMS schicken. Beim Demokonto musst du nur auf „Anfordern“ klicken und es wird automatisch eine TAN generiert. Ändere die TAN zunächst in wexxqx ab. Was passiert? Gib nun die richtige TAN wexxqe ein und sende die Überweisung ab.

- Hat die Überweisung geklappt? Wie kannst du das überprüfen?
- Bei welcher Bank ist Timm?
- Wann wird die Überweisung ausgeführt? (Buchungstermin)
- Schau nun auf die Kontenübersicht. Was hat sich geändert? Wie viel Geld ist noch auf dem Konto?

Skimming

Skimming – was ist das?

Skimming (englischer Begriff) bedeutet soviel wie „Abschöpfen“ oder „Absahnen“.

Der Begriff steht für eine Methode, illegal elektronische Daten von Zahlungskarten (ec-Karte oder Kreditkarte) „auszuspähen“. Dabei setzt sich die Begehungsweise aus zwei strafrechtlich separaten Tatbeständen zusammen:

- Ausspähen/Abfangen von Daten (§ 202a StGB)
- Vorbereitung bzw. Fälschung von Zahlungsmitteln (§§ 152a, 152b StGB i. V. m. § 149 StGB)

Mit den auf diese kriminelle Art erlangten Daten werden Kopien der Geldkarten gefertigt. Damit können die Täter ausschließlich im Ausland Geld von den Konten abheben.

Skimming richtet sich zunächst auf das Ausspähen gespeicherter Daten, die sich auf dem Magnetstreifen der Zahlungskarten befinden. Dies geschieht vor allem durch den Einsatz kleinster elektronischer Bauteile, die rund um die Lesemodule für Zahlungskarten am Geldausgabeautomaten oder anderen Lesegeräten, z. B. an den Eingangstüren, angebracht werden.

Um in den Besitz der Daten auf dem Magnetstreifen zu kommen, installieren die Täter vor dem originalen Karteneinschubschacht zusätzlich ein manipuliertes Aufsatzkartenlesegerät oder vor dem originalen Kartenschacht am Geldausgabeautomaten eine komplette Frontplatte. Diese manipulierten Kartenleser sehen genauso wie der Kartenleser des Geldausgabeautomaten aus und werden so hergestellt, dass die eingeschobene Bankkarte durch das illegale Lesegerät zum originalen Kartenleser weitertransportiert wird. So werden die Kontodaten durch das manipulierte Aufsatzkartenlesegerät ausgelesen und gespeichert. Das Geldabheben am Geldausgabeautomaten verläuft für den Kunden störungsfrei.

Daran schließt sich das Ausspähen der PIN an, wofür die Täter unter Zuhilfenahme von fototechnischen Modulen, z. B. Kamera, Fotohandy, die Eingabe der PIN am Automaten optisch erfassen.

Eine weitere Begehungsart ist die Verwendung einer Aufsatztastatur, die die Eingabe der PIN als elektronischen Impuls erkennt.

Welche Automaten sind betroffen? Wo stehen sie?

Skimming findet vorwiegend in Geld- und Kreditinstituten statt. Aber auch alle anderen Bereiche des unbaren Zahlungsverkehrs, z. B. Einkaufscenter oder Tankstellen, können von Skimming-Straftaten betroffen sein.

Präventionstipps

- Schaut euch den Karteneingabeschlitz der Eingangstür und des Geldausgabeautomaten genau an, bevor ihr die Karte einführt! Im Zweifel solltet ihr das Personal des Geldinstitutes verständigen!
- Schaut euch den Geldausgabeautomaten genau an, ob z. B. eine Leiste zur Aufnahme einer Minikamera angebracht sein könnte! Sie dient der Ausspähung eurer PIN.
- Auch Prospekthalter o. Ä. in Automatennähe könnten eine Minikamera verbergen.
- Schaut euch die Tastatur des Geldausgabeautomaten genau an! Seid misstrauisch, wenn die Tastatur nicht richtig sitzt!
- Sprecht mit eurem Geldinstitut über eine automatische Sperrung eurer Karte für Geldabhebungen im Ausland und vereinbart einen persönlichen Verfügungsrahmen für die Dauer eurer Auslandsreise!

Skimming

Präventionstipps

- Geht immer sorgsam mit eurer Zahlungskarte um und bewahrt die PIN stets getrennt von der Karte auf!
- Wichtig! Verdeckt die Tastatur bei der Eingabe der PIN immer mit der Hand oder z. B. einer Zeitung bei den Kartenleseterminals an den Kassen des Einzelhandels!
- Es wird zum Öffnen einer Eingangstür niemals die PIN abgefragt. Wenn doch, verständigt die Polizei und das Geldinstitut!
- Achtet auf Personen, die sich euch verdächtig nähern (Sicherheitsabstand) und lasst euch nicht ablenken!
- Gebt niemals mehrfach eure PIN ein, auch nicht, wenn euch eine unbekannte Person dazu auffordert!
- Erscheint euch etwas ungewöhnlich, die Karte nicht benutzen, sucht dann ein anderes Geldinstitut auf!
- Kontrolliert regelmäßig eure Kontoauszüge und wendet euch bei Auffälligkeiten sofort an eure Bank!
- Nutzt überwiegend euch bekannte Geldausgabeautomaten möglichst zu Banköffnungszeiten!

Skimming – Unterrichtseinheit

Zielgruppe: ab Klasse 10

Dauer: 1 Zeitstunde

Lernziele:

- Die Schülerinnen und Schüler schulen ihre Fähigkeiten, sich selbstständig anhand von Arbeitsmaterialien Informationen einzuholen und hieraus die wichtigsten Punkte zu filtern.

- Die Schülerinnen und Schüler werden für die Gefahren sensibilisiert und erfahren, worauf sie beim Geldautomaten und beim Bezahlen mit der EC Karte achten müssen.

Materialien:

Selbstgespräch „Skimming“, Flyer „Skimming“, Beamer, Laptop, Boxen, Leinwand

Methoden:

Einzelarbeit, Auswertung im Plenum, Gruppenarbeit

Unterrichtsplanung:

Den Schülerinnen und Schülern wird zu Beginn der Stunde das Selbstgespräch „Skimming“ gezeigt. Sie haben die Aufgabe, wichtige Informationen, die dort gegeben werden, aufzuschreiben. Im Anschluss werden die gesammelten Informationen am Tafelbild zusammengestellt.

Die Schülerinnen und Schüler sollen im nächsten Schritt versuchen, mögliche Präventionstipps zum Thema Skimming für andere Jugendliche zu formulieren.

Die Lehrkraft kann mittels der Informationen, die dazu auf dem Infoflyer „Skimming“ gegeben werden, den Schülerinnen und Schüler wichtige Hinweise und Gedankenstützen mitgeben.

Am Ende können die Ergebnisse der Schülerinnen und Schüler mit dem Flyer verglichen werden.

Hausaufgabenvorschlag:

Die Lehrkraft stellt folgende These auf:

„Fälle von „Skimming“ sind alles nur Einzelfälle und werden von der Presse zusätzlich aufgebauscht!“

Die Schülerinnen und Schüler sollen im Internet recherchieren, wann und wie oft die Medien (z. B. Print) über Skimmingfälle in der Vergangenheit berichtet haben. Welche Artikel findet man dazu? Sie sollen eine Tabelle anlegen, in der sie den Link der Seite vermerken und kurz die Inhalte der Seite beschreiben.

Phishing

Datendiebstahl im Internet

„Phishing" – Was ist das?

„Phishing" kommt vom englischen Wort „fishing" und bedeutet soviel wie „Fischen" oder „Angeln". Dabei wird versucht an sensible Daten wie Passwörter oder PIN-Nummern von Internetbenutzern zu gelangen. Dies geschieht z. B. über gefälschte E-Mails und Webseiten.

Die Täter treten meist in Gruppen auf und nutzen diese geheimen Daten, um an das Geld ihrer Opfer zu gelangen.

Wie machen die Täter das?

Die Täter gehen dabei in zwei Schritten vor: Zuerst werden massenweise E-Mails versandt und damit ein eventuell bestehendes Vertrauensverhältnis ausgenutzt. Diese Mails enthalten meist Aufforderungen weiterführender Links auf gefälschte Webseiten zu folgen und dort vertrauliche Informationen wie Benutzernamen, Passwörter oder PIN-Nummern anzugeben.

Die manipulierten Webseiten sind von den Originalen meist kaum zu unterscheiden, lediglich die Adressen weisen kleine Unterschiede auf und verfügen über kein gültiges Sicherheitszertifikat. Das Sicherheitszertifikat zeigt an, ob man wirklich mit der gewünschten Webseite verbunden ist. Das erkennt ihr an einem grün/blauen Feld mit Zertifikats- und Domaininhaber in der Adressleiste und einem Schlosssymbol in der Statusleiste eures Browsers.

Wenn die Zugangsdaten eines Online-Banking-Accounts gestohlen wurden, können die Täter über das Konto verfügen und Geld ins Ausland überweisen.

Phishing ist aber nicht nur auf das Internet beschränkt, auch telefonisch (Voice Phishing) oder per SMS (SMiShing) können Daten gestohlen werden.

Was kann ich tun, damit mir das nicht passiert?

- Haltet eure Software wie Antivirenprogramme, Firewall, Betriebssystem und Browser auf dem aktuellen Stand!
- Seriöse Unternehmen (z. B. Banken) werden euch nie auffordern, vertrauliche Daten per E-Mail oder Telefon preiszugeben.
- Schaltet in E-Mails und Browsern die Aktivinhalte wie Java-Scripte aus oder stellt sicher, dass ihr vor dem Ausführen immer gefragt werdet!
- E-Mails solltet ihr euch nur im Rein-Text-Format anzeigen, denn HTML-E-Mails lassen sich leicht manipulieren!
- Verwendet für jede Anwendung ein anderes Passwort!
- Phishing-E-Mails kann man manchmal an mangelhafter deutscher Sprache (kyrillische Zeichen, „a" statt „ä" oder „ae") oder namenlose Anrede (Sehr geehrte/r Kunde/in) erkennen.
- Des Weiteren enthalten gefälschte E-Mails oft Drohungen oder signalisieren einen dringenden Handlungsbedarf („Verifizieren Sie Ihre Daten innerhalb der nächsten zwei Tage!").
- Öffnet nur E-Mail-Anhänge von euch bekannten Personen!
- Sichere Webseiten kann man an einem grün/blauen Feld mit Zertifikats- und Domaininhaber in der Adressleiste und einem Schlosssymbol in der Statusleiste im Browser erkennen.

Phishing

- Beim Eingeben vertraulicher Daten stellt sicher, dass die Verbindung verschlüsselt ist! Meist wird der Standard SSL (Secure Sockets Layer) verwendet, dies erkennt ihr daran, dass die URL mit „https“ statt „http“ beginnt.

- Phishing-Webseiten erkennt man daran, dass die Adressen kleine, unübliche Veränderungen oder Zusätze enthalten, wie beispielsweise:
  www.deutsche-bankXY.de

- Überprüft regelmäßig eure Kontoauszüge!

Und was, wenn es mir doch passiert ist?

- Falls ihr den Verdacht habt, Opfer eines Phishing-Angriffs zu sein, wendet euch an das betreffende Unternehmen (z. B. eure Bank)!

- Erstattet außerdem Anzeige bei der Polizei!

Quellen:

CD-ROM „Ins Internet – mit Sicherheit“ – Bundesamt für Sicherheit in der Informationstechnik/
www.bsi-fuer-buerger.de

www.de.wikipedia.org/wiki/phishing

Phishing – Unterrichtseinheit

Schwerpunkt: Sicherheit

Zielgruppe: ab Klasse 10

Dauer: 1 Zeitstunde

Lernziele:

- Die Schülerinnen und Schüler lernen verschiedene Methoden von Phishing kennen, können die Gefahren hierbei abschätzen.
- Die Schülerinnen und Schüler schulen ihre Fähigkeiten, sich selbstständig anhand von Arbeitsmaterialien Informationen einzuholen und hieraus die wichtigsten Punkte zu filtern.
- Die Schülerinnen und Schüler üben kritische Betrachtung von unbekannten Mails und lernen, Inhalte zu hinterfragen.

Materialien:

Tafel, DVD-Player, Fernseher, internetfähige PCs ohne Zugangsbeschränkung (Computerkabinett), AB 1, AB 2, Simple Show „Phishing"

Methoden:

Einzelarbeit, Gruppenarbeit, Gesprächskreis, Diskussionen, Recherche

Unterrichtsplanung:

Zu Beginn der Einheit schauen sich Schüler und Lehrer gemeinsam die Simpleshow „Phishing" an. Im Anschluss daran werden im Plenum die soeben gesehen Inhalte wiederholt.

Fragen können sein:

- Welche Fehler hat Johanna gemacht?
- Wie hätte Sie die Fehler vermeiden können?
- Welche Daten wollten die Gauner warum von Johanna erhalten und wie haben sie das geschafft?
- Haben die Schüler bereits Erfahrungen mit Phishing-Mails gemacht?

Im Anschluss an die Diskussion erhalten die Schüler das Arbeitsblatt 1. Die Schüler erhalten die Aufgabe herauszufinden, ob es sich um eine echte oder gefälschte Mail handelt.

Anschließend werden im Klassenverband die Lösungen diskutiert und besprochen, inwieweit die Schüler selbst schon einmal solche Mails erhalten haben. Darüber hinaus wird hinterfragt, wie sich die Schüler nach Erhalten einer Mail dieser Art verhalten haben.

Anschließend erhalten die Schüler einen Rechercheauftrag. Im Internet unter www.bsi-fuer-buerger.de sollen sie recherchieren, welche weiteren Phishing-Methoden es gibt. Außerdem soll ein Regelkatalog erstellt werden, der aufzeigt, wie man sich am besten vor Phishing schützen kann.

Arbeitsblatt 2 verteilen

Das Arbeitsblatt kann als kleiner Test von der Lehrkraft oder innerhalb der Unterrichtsstunde gemeinsam ausgewertet werden. Eventuelle Fragen der Schüler werden beantwortet.

Phishing

Arbeitsblatt 1

Sieh dir die folgende Mail genau an. Kannst du erkennen, ob es sich bei der Mitteilung um eine echte Mail der Bank oder um eine Phishing-Mail handelt? Woran siehst du das?

Sortware-Aktualisierung

Von: Support-reference@sparkasse.de
An: Timm.Schlau@mail.de
Bcc:
Betreff: Sortware-Aktualisierung

Sehr geehrte Kundin, sehr geehrter Kunde,

Der technische Dienst der Bank führt die planmäßige Aktualisierung der Software durch Fur die Aktualisierung der Kundenbankist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer muessen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.

https://www.sparkasse.de/firmenkunden/B_electronic-banking/online_banking_cud.html

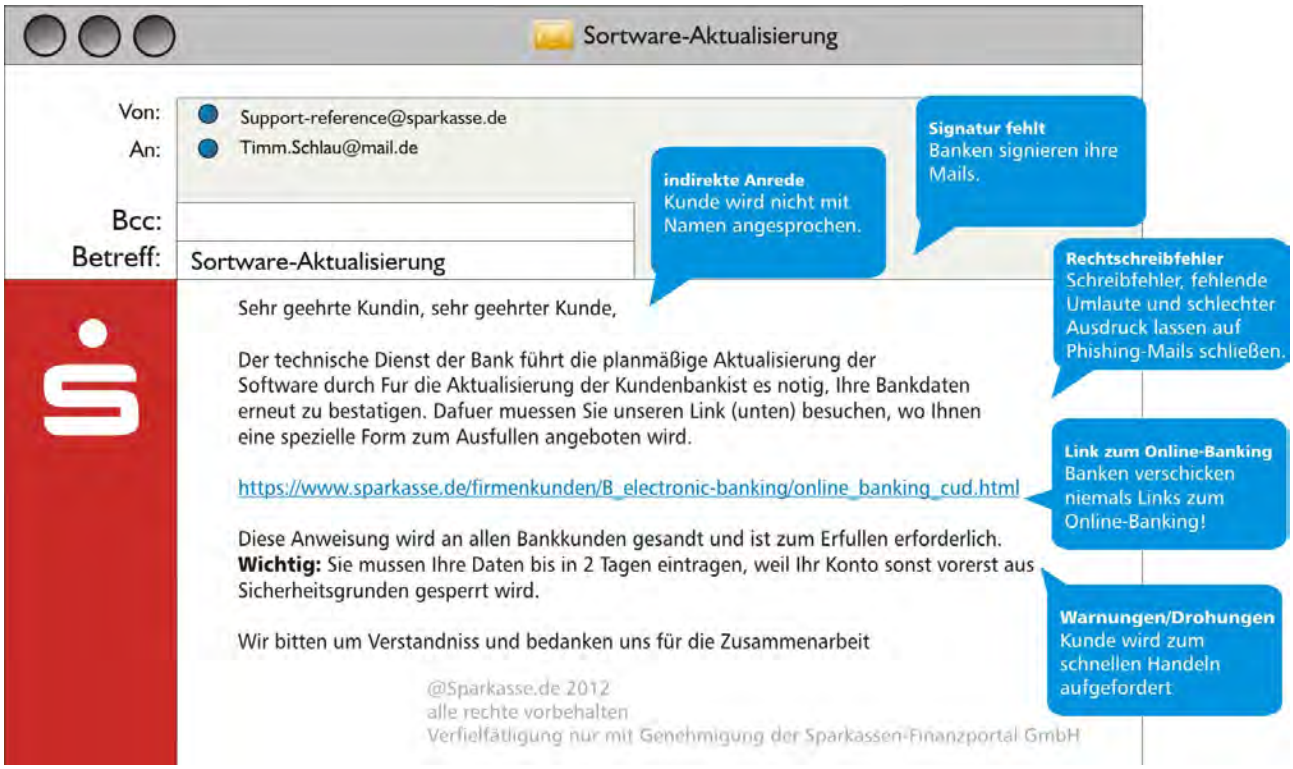
Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.
Wichtig: Sie mussen Ihre Daten bis in 2 Tagen eintragen, weil Ihr Konto sonst vorerst aus Sicherheitsgrunden gesperrt wird.

Wir bitten um Verstandniss und bedanken uns für die Zusammenarbeit

Schreibe hier deine Begründung auf:

Phishing

Lösungen zu Arbeitsblatt 1



Phishing

Arbeitsblatt 2

1. Finde heraus, welche Phishingmethoden es noch gibt und wie die Täter dabei vorgehen!

Methode	Vorgehensweise der Täter

2. Was muss man beachten, um nicht Opfer von Phishing zu werden? Schreibe die Regeln auf!

Online-Shopping

ebay, Amazon und Co.

Wie funktioniert das Einkaufen im Internet?

Mittlerweile gibt es sehr viele Internetkaufhäuser und der Einkauf im Internet wird immer beliebter. Nahezu jeder Händler bietet einen Onlineshop an. Die Nutzung des Angebots im Internet einzukaufen, zieht sich durch alle Generationen und alle Lebensbereiche. Online-Shopping ist eine beliebte und bequeme Möglichkeit, Waren aller Art zu kaufen, jedoch birgt es auch verschiedene Risiken in sich.

Die Bezahlung bei einem Interneteinkauf ist dabei eine schwierige Angelegenheit:

Es gibt die herkömmlichen Zahlungsmethoden wie Überweisungen, Lastschriftabbuchungen und Zahlungen per Nachnahme und es gibt speziell für den Onlinekauf entwickelte Zahlungsfunktionen.

Prepaid-Karten

Diese funktionieren wie Telefonwertkarten. Hierbei rubbelt ihr einen PIN-Code frei und könnt über die Internetseite des Kartenanbieters auf euer Guthaben zugreifen. Zusätzlich schützt ihr eure Daten mit einem Passwort.

PayPal

Das ist ein spezielles Angebot von „ebay“, aber auch in zahlreichen anderen Internetshops verfügbar, bei dem ihr euch ein virtuelles Konto einrichten könnt (www.paypal.de). Darüber können dann die Onlinegeschäfte abgewickelt werden und die Zahlungen für ersteigerte Waren geht noch schneller vonstatten. Ihr als Nutzer könnt entweder über Kreditkarte oder Lastschrift euer PayPal-Konto ausgleichen. Es besteht auch die Möglichkeit, mittels Überweisung ein Guthaben auf das Konto einzuzahlen, das dann für Transaktionen genutzt werden kann.

Komplettsysteme für Onlinebezahlung

Bei der Firma Firstgate könnt ihr euch ein sogenanntes Surferkonto einrichten. Hierfür müsst ihr persönliche Daten wie Namen, Wohnort, Bankverbindung und E-Mail-Adresse angegeben. Dann kann man bei allen Partnern der betreffenden Firma einkaufen und ihr zahlt am Ende per Sammelrechnung.

Auf welche Gefahren muss ich dabei achten?

Da man im Internet weitestgehend anonym unterwegs ist, sind Betrüger auch schwer zu verfolgen. Besonders unangenehm sind die Praktiken der Phisher. Diese wollen mit Hilfe gefälschter E-Mails, Internetnutzer dazu bewegen, ihre Kundendaten preiszugeben. Zudem ist bei im Ausland erworbenen Produkten damit zu rechnen, dass Einfuhrzölle entrichtet werden müssen.

Die goldene Regel beim Onlinekauf lautet: Lieber mehr Zeit in das Lesen der allgemeinen Geschäftsbedingungen investieren, als sich danach über missglückte Geschäfte ärgern!

Wie kann ich mich schützen?

- Überprüft, ob es sich um einen seriösen Anbieter im Internet handelt und lest die allgemeinen Geschäftsbedingungen (AGB)! Achtet auch darauf, dass neben den elektronischen Kontaktdaten auch Adresse und Telefonnummern angegeben sind!

- Eure Daten müssen immer verschlüsselt übertragen werden! Das erkennt ihr am „https“ in der Internetadresse. Oft erscheinen auch ein Sicherheitsschloss oder ein Schlüssel als Symbole in der Statusleiste.

- Speichert wichtige Daten und Unterlagen zusätzlich auf externen Speichermedien, damit sie nicht verloren gehen!

Online-Shopping

- Speichert keine Passwörter, PIN, TAN oder andere Zugangscodes auf eurem Rechner! Bewahrt eure PIN und das Passwort nie gemeinsam an einem Ort auf!
- Verzichtet auf das Ausführen „aktiver Inhalte“ und stellt euren Browser so ein, dass JavaScript nicht automatisch ausgeführt wird!
- Verwendet beim Surfen im Internet immer eine Firewall und ein Virenschutzprogramm!
- Schaut nach, ob es auch alternative Bestellmöglichkeiten gibt, etwa per Telefon oder Fax!
- Seid vorsichtig, wenn ihr E-Mails erhaltet, in denen ihr aufgefordert werdet, eure persönlichen Daten zu aktualisieren! Betrüger können auf diese Weise versuchen, euch auf gefälschte Seiten von Unternehmen wie Banken zu locken, um euch persönliche Informationen zu entlocken.

Quelle:

CD-ROM „Ins Internet – mit Sicherheit“ – Bundesamt für Sicherheit in der Informationstechnik/
www.bsi-fuer-buerger.de

Online-Shopping – Unterrichtseinheit

Zielgruppe: ab Klasse 9

Dauer: 3 Zeitstunden

Lernziele:

- Die Schülerinnen und Schüler sollen ein kritisches Verbraucherverhalten bei der Nutzung des Internets entwickeln.

- Die Schülerinnen und Schüler recherchieren im Internet worauf bei Onlineeinkäufen zu achten ist, sie vergleichen Angebote im Geschäft mit denen im Internet und lernen die Risiken bei Onlineeinkäufen kennen und richtig einzuordnen.

Methoden:

Einzelarbeit, Gruppenarbeit

Materialien:

Arbeitsblatt 1 „Einkaufen im Internet", Simple Show und/oder Selbstgespräch, internetfähige Rechner ohne Zugangsbeschränkung

Unterrichtsplanung:

Zu Beginn der Einheit ist es für die Lehrkraft wichtig zu wissen, wer von den Schülerinnen und Schülern schon im Internet etwas eingekauft hat und welche Erfahrungen die Jugendlichen dabei gemacht haben. Dafür können Sie eine kleine Umfrage in der Klasse durchführen und sich darüber im Gespräch austauschen. Hier kommt gewiss die Frage nach der Geschäftsfähigkeit auf.

Dieser soll im nächsten Schritt nachgegangen werden. Wer kann im Internet einkaufen? Wie sieht die Rechtslage aus? Dazu recherchieren die Schülerinnen und Schüler im Internet und füllen die Tabelle auf dem Arbeitsblatt 1 aus. In diesem Zusammenhang kann auch geklärt werden was der Taschengeldparagraf (§ 110 BGB) besagt.

Im Folgenden Unterrichtsverlauf wird die Simpleshow zum Thema „Einkaufen im Internet" gezeigt. Die Schülerinnen und Schüler haben die Aufgabe, sich während der Show Notizen zu den Inhalten zu machen. Sie sollen herausarbeiten, welche Risiken genannt werden. Parallel kann auch das „Selbstgespräch" als filmisches Element eingesetzt werden. Hierin wird ebenfalls auf Risiken bei Interneteinkäufen eingegangen.

Im Anschluss erhalten die Schülerinnen und Schüler eine Rechercheaufgabe für das Internet. Sie sollen auf der Seite der Verbraucherzentrale Sachsen/Anhalt (www.verbraucherzentrale-sachsen-anhalt.de) nach Informationen zu diesem Thema suchen und diese herausarbeiten. Mit den Materialien wird eine Checkliste mit dem Titel „Woran erkenne ich einen guten Onlineshop" entwickelt. Folgende Stichworte können Sie den Schülerinnen und Schüler geben: Preise, Rechnungen, Datensicherheit, Anbieter/Website, Widerruf, Rücksendekosten, Rückgaberecht.

Für die Gestaltung ist ein A5 Format denkbar, was in der Schule zu einem Informationstag verteilt werden kann.

Hausaufgabenvorschlag:

Die Schülerinnen und Schüler sollen bestimmte Produkte (z. B. Kleidung, Elektronik) im Onlineshop mit denen im Geschäft vergleichen. Zusätzlich sollen die Vor- und Nachteile für beide Verkaufsorte herausgearbeitet werden.

Online-Shopping

Arbeitsblatt 1

Bitte trage die richtigen Antworten in die freien Feldere ein.

Geschäftsfähigkeit	**Alter**	**Art/Umfang der Käufe**
nicht geschäftsfähig		
beschränkt geschäftsfähig		
geschäftsfähig		

Was besagt der Taschengeldparagraf (§ 110 BGB)?

Online-Shopping

Lösungen zu Arbeitsblatt 1:

Bitte trage die richtigen Antworten in die freien Feldere ein.

Geschäftsfähigkeit	**Alter**	**Art/Umfang der Käufe**
nicht geschäftsfähig	unter 7 Jahre	dürfen nicht einkaufen, dies müssen die Erziehungsberechtigten tun.
beschränkt geschäftsfähig	7 bis 18 Jahre	nur in der Höhe des Taschengeldes
geschäftsfähig	ab 18 Jahren	uneingeschränkter Umfang

Was besagt der Taschengeldparagraf (§ 110 BGB)?

Ein von dem Minderjährigen ohne Zustimmung des gesetzlichen Vertreters geschlossener Vertrag gilt als von Anfang an wirksam, wenn der Minderjährige die vertragsmäßige Leistung mit Mitteln bewirkt, die ihm zu diesem Zweck oder zu freier Verfügung von dem Vertreter oder mit dessen Zustimmung von einem Dritten überlassen worden sind.

Soziale Netzwerke

studiVZ, facebook & Co.

In sozialen Netzwerken (englisch: „Social Communities“ oder „Social Networks“) hat man die Möglichkeit, eigene Inhalte in Text und Bild zu veröffentlichen, sich mit anderen zu vernetzen und im Gegenzug auf Veröffentlichungen der anderen in Form von Texten und Bildern zu reagieren. Des Weiteren können Freundeslisten angelegt werden und man kann Informationen austauschen. Über verschiedene Kommunikationswege (z. B. Chats, Foren) im Internet hat jeder die Möglichkeit, mit anderen Menschen in Kontakt zu treten.

Gefahren in sozialen Netzwerken

Offenlegung persönlicher Daten

Die Preisgabe von persönlichen Daten (E-Mail-Adressen, Telefonnummern, etc.) kann von Firmen missbräuchlich genutzt werden, um die Nutzer mit Werbung zu bombardieren. Auch die Voreinstellungen zum Schutz der Privatsphäre sind bei der Registrierung oft nicht ausreichend vorgenommen, so dass alle eingestellten Daten auch für andere sofort sichtbar sind. Ebenfalls ist darauf zu achten, dass potentielle Arbeitgeber in den sozialen Netzwerken nach Informationen ihrer Bewerber suchen. Freizügige Fotos können dabei ein Ausschlusskriterium sein. Einmal eingestellte Daten können von Dritten auf deren Computer archiviert und so auf anderen Seiten im Internet verwendet werden.

Phishing

Über gefälschte Webseiten versuchen Betrüger an die Zugangsdaten für soziale Netzwerke heranzukommen. Über Links in einer E-Mail gelangen die Nutzer auf eine Seite, die der des sozialen Netzwerks täuschend ähnlich sieht. Versuchen Sie sich dort einzuloggen, können die Betrüger Nutzername und Passwort abfischen und haben ab dann vollen Zugriff auf den Account, können Daten einsehen und ändern, Nachrichten verschicken und chatten. Die Freunde merken davon nichts und denken, alle Änderungen und Nachrichten kämen von der bekannten Person.

Identitätsdiebstahl

Kriminelle versuchen zunehmend, bestehende Nutzer-Accounts zu hacken, um deren Identitäten für ihre Betrügereien zu nutzen. Oftmals täuschen diese Hacker nach Übernahme eines Accounts eine Notsituation vor und bitten die vernetzen Freunde um finanzielle Hilfe. Das über das Nutzerprofil erlesene Wissen kann dazu beitragen, das Vertrauen zu untermauern und Freunde zu täuschen.

„Unechte“ Profile werden zunehmend dazu genutzt, Personen zu schaden: Diebe können so zum Beispiel ausspionieren, wann jemand im Urlaub ist und die Wohnung leer steht.

Mobbing

Soziale Netzwerke haben Mobbing auf eine neue Ebene gebracht. Freundschaften sind in sozialen Netzwerken schneller geschlossen als in der „realen“ Welt. So gelangen Informationen an Personen, die diesen sonst vielleicht nicht anvertraut worden wären. Wer böswillige Absichten hat, kann diese Informationen dafür nutzen, um jemanden bewusst bloßzustellen oder gegen ihn zu intrigieren. So genannte „Cyberstalker“ können sich „unechte“ Profile anlegen, in denen sie sich als eine reelle oder fiktive andere Person ausgeben. So können sie in vollkommener Anonymität andere Personen über das soziale Netzwerk belästigen.

Verbreitung von Schadsoftware

Das Vertrauen der Nutzer in die sozialen Netzwerke ist meist groß. Betrüger haben deshalb eine gewohnte Masche auf diese Plattformen übertragen: Sie verschicken Nachrichten, die einen Link auf manipulierte Webseiten enthalten. Über diese Seiten werden dann Schadprogramme (z. B. Viren oder Trojaner) verbreitet. Manche soziale Netzwerke bieten Zusatzanwendungen (z. B. Mini-Spiele) an, die Nutzer ihrem Profil hinzufügen können. Problematisch ist, dass diese Anwendungen von Drittanbietern stammen, deren Sicherheitsstandards nicht zwangsläufig denen der sozialen Netzwerke entsprechen müssen.

Soziale Netzwerke

Tipps zum sicheren Umgang mit sozialen Netzwerken

- Seien Sie zurückhaltend mit der Preisgabe persönlicher Informationen!
- Erkundigen Sie sich über die allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des genutzten sozialen Netzwerks!
- Seien Sie wählerisch bei Kontaktanfragen – Kriminelle „sammeln" Freunde, um Personen zu schaden!
- Melden Sie „Cyberstalker", die Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren!
- Verwenden Sie für jede Internetanwendung, insbesondere auch wenn Sie in verschiedenen sozialen Netzwerken angemeldet sind, ein unterschiedliches und sicheres Passwort!
- Geben Sie keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis!
- Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Netzwerke an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen!
- Wenn Sie „zweifelhafte" Anfragen von Bekannten erhalten, erkundigen Sie sich außerhalb sozialer Netzwerke nach der Vertrauenswürdigkeit dieser Nachricht!
- Klicken Sie nicht wahllos auf Links – soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben!
- Sprechen Sie mit Ihren Kindern über deren Aktivitäten in sozialen Netzwerken und klären Sie sie über die Gefahren auf!

Quelle:

www.bsi-fuer-buerger.de

Online-Banking

Online-Banking – was ist das?

Mit dem Begriff "Online-Banking" wird die Abwicklung von Bankgeschäften über das Internet bezeichnet. Die Angebotspalette reicht vom bloßen Abfragen des Kontostands oder einzelner Umsätze über das Überweisen sowie Einrichten von Daueraufträgen bis hin zu individuellen Auswertungen der Kontobewegungen.

Online-Banking ist für viele Menschen heute ganz selbstverständlich. Jedoch gilt auch beim Online-Banking zu beachten, dass Kriminelle versuchen, Konto- und Kreditkartendaten der Nutzer auszuspähen (Phishing) und somit an deren Geld zu kommen.

Funktionsweise von Online-Banking

Online-Banking wird über das Internet angeboten. Die von den Banken verwendeten Verbindungen werden heute üblicherweise über SSL (Secure Sockets Layer) verschlüsselt angeboten. Dies erkennen Sie daran, dass die URL mit „https" statt „http" beginnt.

Der Zugang zum persönlichen Konto erfolgt zumeist über das PIN/TAN-System. Dabei gibt der Benutzer neben seiner Kontonummer eine persönliche Identifikationsnummer (PIN) ein. Eine Aktion – etwa die Änderung dieser Daten oder eine Überweisung – kann jedoch erst mit Eingabe einer Transaktionsnummer (TAN) getätigt werden. Die TAN ist dabei nur einmal gültig und kann nicht wiederverwendet werden.

Verschiedene Verfahren:

iTAN

Die TANs auf der Liste sind durchnummeriert (indiziert). Wenn eine Transaktion erfolgt ist, wird eine bestimmte TAN (z. B. Nr. 31) auf Ihrer Liste abgefordert, diese ist an den aktuellen Auftrag gebunden und kann nicht beliebig verwendet werden.

mTAN oder SMSTAN

Hierbei haben sie keine seperate TAN-Liste in den Händen, sondern es wird bei jeder Transaktion eine sogenannte „mobile TAN" als SMS auf Ihr Handy geschickt. Diese TANs haben eine zeitlich begrenzte Gültigkeit, d. h. sie müssen umgehend benutzt werden. Der Nachteil bei diesem Verfahren ist, dass zusätzliche Kosten für die Übertragen der TAN per SMS auf Sie zu kommen können.

chipTAN-Verfahren

Bei diesem Verfahren erhalten Sie von Ihrer Bank einen TAN-Generator mit Ziffernfeld und Karteneinschub, auf dessen Rückseite zusätzlich fünf optische Sensoren angebracht sind. Nach Eingabe einer Transaktion – etwa einer Überweisung – erscheint auf dem PC-Bildschirm eine Grafik mit fünf flackernden schwarzweißen Flächen. Sie müssen nun Ihre Bankkarte in den Generator stecken und diesen an die Grafik auf dem Monitor halten. Von dort aus werden Informationen als Lichtsignale an den Generator übertragen, der in seinem Display danach die Kontonummer des Empfängers und den Überweisungsbetrag anzeigt. Nachdem der Kunde diese bestätigt hat, errechnet der Generator eine TAN.

Sicherheitstipps

- Setzen Sie Verschlüsselungen ein!
- Schützen Sie sensible Daten bei der Übertragung über offene Netze. Vergewissern Sie sich zudem, dass die Datenübertragung, etwa bei WLAN-Verbindungen, ausreichend verschlüsselt ist!
- Beim Eingeben vertraulicher Daten stellen Sie sicher, dass die Verbindung verschlüsselt ist! Meist wird der Standard SSL (Secure Sockets Layer) verwendet, dies erkennen Sie daran, dass die URL mit „https" statt „http" beginnt.

Online-Banking

Sicherheitstipps

- Wählen Sie als Passwort eine schwer zu erratende Buchstaben-/Zahlenkombinationen, schützen Sie diese Zugangsdaten vor Dritten und speichern Sie diese niemals ab!
- Betreiben Sie Online-Banking soweit möglich nur von eigenen Geräten aus!
- Achten Sie darauf, keine Software aus unseriösen oder unsicheren Quellen auf Ihrem Computer zu speichern!
- Schützen Sie Ihren PC vor unerlaubten Zugriffen!
- Setzen Sie aktuelle Virenschutzsoftware und Firewalls ein!
- Spielen Sie aktuelle Sicherheitsupdates für Ihr Betriebssystem ein!
- Überprüfen Sie regelmäßig Ihre Kontoauszüge und wenden Sie sich bei Auffälligkeiten sofort an Ihre Bank!
- Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Online-Banking!
- Reagieren Sie nicht auf Phishing-Mails!
- Sperren Sie Ihren Online-Banking-Zugang, wenn Ihnen etwas verdächtig vorkommt!

Im Ernstfall

Wenn Sie den Eindruck oder den Verdacht haben, dass etwas nicht stimmt, sollten Sie sofort aktiv werden:

- Sperren Sie unverzüglich Ihr Bankkonto und Ihren Zugang zum Online-Banking! Am schnellsten geht das, indem Sie zum Beispiel die Anmeldemaske zum Online-Banking aufrufen und dreimal hintereinander die falsche PIN eingeben. Oder rufen Sie den zentralen Sperr-Notruf 116 116 (aus dem Ausland +49 116 116) an und lassen Sie Ihren Zugang telefonisch sperren!
- Danach wenden Sie sich sofort an Ihre Bank und melden die Auffälligkeiten! Gegebenenfalls besteht die Möglichkeit, Kontobewegungen rückgängig zu machen.
- Prüfen Sie umgehend die Kontoumsätze anhand des Papierauszuges!
- Sollten Sie Opfer eines Phishing-Angriffs mittels eines Trojaners geworden sein, müssen Sie Ihren PC fachgerecht von der Schadsoftware befreien!
- Erstatten Sie Anzeige bei der Polizei!

Quelle:

CD-ROM „Ins Internet – mit Sicherheit“ – Bundesamt für Sicherheit in der Informationstechnik/
www.bsi-fuer-buerger.de

Skimming

Skimming – was ist das?

Skimming (englischer Begriff) bedeutet soviel wie „Abschöpfen“ oder „Absahnen“.

Der Begriff steht für eine Methode, illegal elektronische Daten von Zahlungskarten (ec-Karte oder Kreditkarte) „auszuspähen“. Dabei setzt sich die Begehungsweise aus zwei strafrechtlich separaten Tatbeständen zusammen:

- Ausspähen/Abfangen von Daten (§ 202a StGB)
- Vorbereitung bzw. Fälschung von Zahlungsmitteln (§§ 152a, 152b StGB i. V. m. § 149 StGB)

Mit den auf diese kriminelle Art erlangten Daten werden Kopien der Geldkarten gefertigt. Damit können die Täter ausschließlich im Ausland Geld von den Konten abheben.

Skimming richtet sich zunächst auf das Ausspähen gespeicherter Daten, die sich auf dem Magnetstreifen der Zahlungskarten befinden. Dies geschieht vor allem durch den Einsatz kleinster elektronischer Bauteile, die rund um die Lesemodule für Zahlungskarten am Geldausgabeautomaten oder anderen Lesegeräten, z. B. an den Eingangstüren, angebracht werden.

Um in den Besitz der Daten auf dem Magnetstreifen zu kommen, installieren die Täter vor dem originalen Karteneinschubschacht zusätzlich ein manipuliertes Aufsatzkartenlesegerät oder vor dem originalen Kartenschacht am Geldausgabeautomaten eine komplette Frontplatte. Diese manipulierten Kartenleser sehen genauso wie der Kartenleser des Geldausgabeautomaten aus und werden so hergestellt, dass die eingeschobene Bankkarte durch das illegale Lesegerät zum originalen Kartenleser weitertransportiert wird. So werden die Kontodaten durch das manipulierte Aufsatzkartenlesegerät ausgelesen und gespeichert. Das Geldabheben am Geldausgabeautomaten verläuft für den Kunden störungsfrei.

Daran schließt sich das Ausspähen der PIN an, wofür die Täter unter Zuhilfenahme von fototechnischen Modulen, z. B. Kamera, Fotohandy, die Eingabe der PIN am Automaten optisch erfassen.

Eine weitere Begehungsart ist die Verwendung einer Aufsatztastatur, die die Eingabe der PIN als elektronischen Impuls erkennt.

Welche Automaten sind betroffen? Wo stehen sie?

Skimming findet vorwiegend in Geld- und Kreditinstituten statt. Aber auch alle anderen Bereiche des unbaren Zahlungsverkehrs, z. B. Einkaufscenter oder Tankstellen, können von Skimming-Straftaten betroffen sein.

Präventionstipps

- Schauen Sie sich den Karteneingabeschlitz der Eingangstür und des Geldausgabeautomaten genau an, bevor Sie die Karte einführen! Im Zweifel sollten Sie das Personal des Geldinstitutes verständigen!
- Schauen Sie sich den Geldausgabeautomaten genau an, ob z. B. eine Leiste zur Aufnahme einer Minikamera angebracht sein könnte! Sie dient der Ausspähung Ihrer PIN.
- Auch Prospekthalter o. Ä. in Automatennähe könnten eine Minikamera verbergen.
- Schauen Sie sich die Tastatur des Geldausgabeautomaten genau an! Seien Sie misstrauisch, wenn die Tastatur nicht richtig sitzt!
- Sprechen Sie mit Ihrem Geldinstitut über eine automatische Sperrung Ihrer Karte für Geldabhebungen im Ausland und vereinbaren Sie einen persönlichen Verfügungsrahmen für die Dauer Ihrer Auslandsreise.

Skimming

Präventionstipps

- Gehen Sie sorgsam mit Ihren Zahlungskarten um und bewahren Sie die PIN stets getrennt von der Karte auf!
- Wichtig! Verdecken Sie die Tastatur bei der Eingabe der PIN immer mit der Hand oder z. B. einer Zeitung bei den Kartenleseterminals an den Kassen des Einzelhandels!
- Es wird zum Öffnen einer Eingangstür niemals die PIN abgefragt. Wenn doch, verständigen Sie die Polizei und das Geldinstitut!
- Achten Sie auf Personen, die sich Ihnen verdächtig nähern (Sicherheitsabstand) und lassen Sie sich nicht ablenken!
- Geben Sie niemals mehrfach Ihre PIN ein, auch nicht, wenn Sie eine unbekannte Person dazu auffordert!
- Erscheint Ihnen etwas ungewöhnlich, die Karte nicht benutzen, suchen Sie dann ein anderes Geldinstitut auf!
- Kontrollieren Sie regelmäßig Ihre Kontoauszüge und wenden Sie sich bei Auffälligkeiten sofort an Ihre Bank!
- Nutzen Sie überwiegend Ihnen bekannte Geldausgabeautomaten möglichst zu Banköffnungszeiten!

Phishing

Datendiebstahl im Internet

„Phishing" – was ist das?

„Phishing"(vom Englischen „fishing") bedeutet soviel wie „Fischen" oder „Angeln". Dabei wird versucht an sensible Daten wie Passwörter oder PIN-Nummern von Internetnutzern zu gelangen. Dies geschieht zum Beispiel über gefälschte E-Mails und Webseiten.

Die Täter, meist organisierte Gruppen, nutzen diese sensiblen Daten, um sich mit einer falschen Identität Geld zu Lasten des Opfers zu beschaffen.

Arbeitsweise der Täter

Üblicherweise gehen die Täter in zwei Schritten vor: Zuerst versenden sie massenweise E-Mails, die den Seiten von Banken oder bekannten Web-Shops sehr ähnlich sehen. Die Nachrichten enthalten meist die Aufforderung, weiterführende Links auf nahezu perfekt gefälschte Webseiten zu folgen und dort vertrauliche Informationen, wie Benutzernamen, Passwörter oder PIN-Nummern anzugeben.

Die manipulierten Webseiten sind von den Originalen meist kaum zu unterscheiden, lediglich die Adressen weisen kleine Unterschiede auf und verfügen über kein gültiges Sicherheitszertifikat. Das Sicherheitszertifikat zeigt an, ob man wirklich mit der gewünschten Webseite verbunden ist. Das erkennen Sie an einem grün/blauen Feld mit Zertifikats- und Domaininhaber in der Adressleiste und einem Schlosssymbol in der Statusleiste Ihres Browsers.

Wenn so die Zugangsdaten eines Online-Banking-Accounts gestohlen wurden, können die Täter über das Konto verfügen und Geld ins Ausland überweisen.

Phishing ist aber nicht nur auf das Internet beschränkt, auch telefonisch (Voice Phishing) oder per SMS (SMiShing) können Daten ausgespäht werden.

Präventionstipps

- Halten Sie Ihre Software wie Antivirenprogramme, Firewall, Betriebssystem und Browser auf dem aktuellen Stand!
- Seriöse Unternehmen werden Sie nie auffordern, vertrauliche Daten per E-Mail oder Telefon preiszugeben.
- Schalten Sie in E-Mails und Browsern die Aktivinhalte wie Java-Scripte aus oder stellen Sie sicher, dass Sie vor dem Ausführen immer gefragt werden!
- Lassen Sie sich E-Mails nur im Rein-Text-Format anzeigen, HTML-E-Mails lassen sich leicht manipulierten!
- Verwenden Sie für jede Anwendung ein anderes Passwort!
- Phishing-E-Mails kann man manchmal an mangelhafter deutscher Sprache (kyrillische Zeichen, „a" statt „ä" oder „ae") oder namenloser Anrede (Sehr geehrte/r Kunde/in) erkennen.
- Gefälschte E-Mails enthalten oft Drohungen oder signalisieren einen dringenden Handlungsbedarf („Verifizieren Sie Ihre Daten innerhalb der nächsten zwei Tage!").
- Öffnen Sie nur E-Mail-Anhänge von Ihnen vertrauten Personen! In anderen Fällen verfolgen Sie keine dort enthaltenen Links.
- Sichere Webseiten kann man an einem grün/blauen Feld mit Zertifikats- und Domaininhaber in der Adressleiste und einem Schlosssymbol in der Statusleiste Ihres Browsers erkennen.

Phishing

- Beim Eingeben vertraulicher Daten stellen Sie sicher, dass die Verbindung verschlüsselt ist! Meist wird der Standard SSL (Secure Sockets Layer) verwendet, dies erkennen Sie daran, dass die URL mit „https“ statt „http“ beginnt.

Im Ernstfall

- Phishing-Webseiten erkennen Sie daran, dass die Adressen kleine, unübliche Veränderungen oder Zusätze enthalten wie beispielsweise:
  www.deutsche-bankXY.de

- Überprüfen Sie regelmäßig Ihre Kontoauszüge auf Auffälligkeiten!

- Falls Sie den Verdacht haben, Opfer eines Phishing-Angriffs zu sein, wenden Sie sich an das betreffende Unternehmen (z. B. Ihre Bank), bei tatsächlich entstandenem Schaden kontaktieren Sie die Polizei!

Quelle:

CD-ROM „Ins Internet – mit Sicherheit“ – Bundesamt für Sicherheit in der Informationstechnik/
www.bsi-fuer-buerger.de

Online-Shopping

ebay, Amazon und Co.

Einkaufen im Internet

Amazon, ebay, Zalando – inzwischen gibt es unzählige Internetkaufhäuser und nahezu jeder Händler bietet einen Onlineshop an. Das Shoppen im Internet wird immer beliebter – ein Trend, der sich durch alle Generationen und Lebensbereiche zieht. Online-Shopping ist vor allem bequem, jedoch birgt es auch verschiedene Risiken in sich.

Die Bezahlung bei einem Web-Einkauf ist eine komplexe Angelegenheit:

Neben den herkömmlichen Zahlungsmethoden, wie Überweisungen, Lastschriftabbuchungen und Zahlungen per Nachnahme gibt es speziell für den Onlinekauf entwickelte Zahlungsfunktionen.

Prepaid-Karten

Diese funktionieren wie Telefonwertkarten. Sie rubbeln einen PIN-Code frei und können über die Internetseite des Kartenanbieters auf Ihr Guthaben zugreifen. Zusätzlich schützen Sie Ihre Daten mit einem Passwort.

PayPal

Das ist ein spezielles Angebot von „ebay“ aber auch in zahlreichen anderen Internetshops verfügbar, bei dem sich der Kunde ein virtuelles Konto einrichten kann (www.paypal.de). Darüber können dann die Onlinegeschäfte abgewickelt werden und die Zahlungen für ersteigerte Waren geht noch schneller vonstatten. Die Nutzer können entweder über Kreditkarte oder Lastschrift ihr PayPal-Konto ausgleichen. Es besteht auch die Möglichkeit, mittels Überweisung ein Guthaben auf das Konto einzuzahlen, das dann für Transaktionen genutzt werden kann.

Komplettsysteme für Onlinebezahlung

Bei der Firma Firstgate kann sich ein Nutzer ein sogenanntes Surfer-Konto einrichten. Hierfür müssen persönliche Daten wie Namen, Wohnort, Bankverbindung und E-Mail-Adresse angegeben werden. Dann kann man bei allen Partnern der betreffenden Firma einkaufen und zahlt am Ende per Sammelrechnung.

Gefahren

Da man im Internet weitestgehendd anonym unterwegs ist, sind Betrüger auch schwer zu verfolgen. Besonders unangenehm sind die Praktiken der Phisher. Diese wollen mit Hilfe gefälschter E-Mails Internetnutzer dazu bewegen, ihre Kundendaten preiszugeben. Zu dem ist bei im Ausland erworbenen Produkten damit zu rechnen, dass Einfuhrzölle entrichtet werden müssen.

Vorsichtsmaßnahmen

- Überprüfen Sie, ob es sich um einen seriösen Anbieter im Internet handelt und lesen Sie die allgemeinen Geschäftsbedingungen (AGB)! Prüfen Sie auch, ob neben den elektronischen Kontaktdaten auch Adresse und Telefonnummern angegeben sind!

- Achten Sie darauf, dass Ihre Daten verschlüsselt übertragen werden! Das erkennen Sie am „https“ in der Internetadresse. Oft erscheinen auch ein Sicherheitsschloss oder ein Schlüssel als Symbol in der Statusleiste.

- Stellen Sie sicher, dass Ihre Daten bei technischen Schäden auf Ihrem PC nicht verloren gehen und speichern Sie wichtige Unterlagen zusätzlich auf externen Speichermedien.

Online-Shopping

- Speichern Sie keine Passwörter, PIN, TAN oder andere Zugangscodes auf ihrem Rechner. Bewahren Sie niemals Ihre Zugangsdaten, wenn sie aus zwei Teilen bestehen (PIN und Passwort), gemeinsam an einem Ort auf.

- Verzichten Sie auf das Ausführen „aktiver Inhalte“ und stellen Sie Ihren Browser so ein, dass JavaScript nicht automatisch ausgeführt wird!

- Verwenden Sie beim Surfen im Internet immer eine Firewall und ein Virenschutzprogramm!

- Prüfen Sie, ob alternative Bestellmöglichkeiten existieren, etwa per Telefon oder Fax!

- Seien Sie vorsichtig, wenn Sie E-Mails erhalten, in denen Sie zur Aktualisierung Ihrer Kundendaten aufgefordert werden! Sogenannte Phisher versuchen auf diese Weise, Sie auf gefälschte Seiten von Unternehmen wie Banken zu locken und Ihnen persönliche Informationen zu entlocken.

Die goldene Regel beim Onlinekauf lautet: Lieber mehr Zeit in das Lesen der allgemeinen Geschäftsbedingungen investieren, als sich danach über missglückte Geschäfte ärgern!

Quelle:

CD-ROM „Ins Internet – mit Sicherheit“ – Bundesamt für Sicherheit in der Informationstechnik/
www.bsi-fuer-buerger.de

ADHS DEUTSCHLAND e.V.
Selbsthilfe für Menschen mit ADHS
Vormals BV AÜK e. V. und BV-AH e. V.

Regionalgruppe Helmstedt
Monika Lehmann
Ostendorf 13
38350 Helmstedt
Tel: 05351 40390, Fax: 05351 2862
rg.helmstedt@adhs-deutschland.de

Presseartikel
Immer mehr Menschen mediensüchtig

Helmstedt, den 03.08.10

Immer mehr Menschen werden in Deutschland nach Einschätzung von Experten vom Internet und von Computerspielen abhängig. Gerade Heranwachsende sind hiervon besonders betroffen. Oft wird der Computer zum besten Freund des Kindes. Je jünger der Nutzer ist, desto anfälliger ist er, eine Suchterkrankung zu entwickeln. Heutzutage sind 98 % der Jungen und Mädchen zwischen 12 und 19 Jahren vernetzt, so Theo Wessel vom Gesamtverband für Suchtkrankenhilfe Berlin.

Dr. med. Bert te Wildt, Facharzt für Psychiatrie und Psychotherapie der Medizinischen Hochschule Hannover (MHH) wird am Mittwoch, dem 8. September, zum Thema „Jugendliche @ Cyberspace“ referieren. Veranstaltungsort ist das Kloster St. Ludgerus, Am Ludgerihof 1 in Helmstedt. Uhrzeit: 19:00 – 21:30 Uhr.

Ursprünglich war das Internet als Informationsquelle gedacht. Selbstverständlich wird es noch immer in dieser Funktion genutzt. Sei es für eine Reiseauskunft oder für schulische Belange, das Internet weiß alles. Inzwischen ist der Computer jedoch oft zum Ersatz des wirklichen Lebens geworden. In „Second Life“ werden, ähnlich wie im echten Leben, Tagesabläufe durchlebt, so dass für manche Spieler die virtuelle Welt unbemerkt zum Ersatz der Realität wird. Eltern fühlen sich oft machtlos in der (Medien-) Erziehung. Häufige Ermahnungen nutzen nichts.

Wo liegt jedoch der Reiz bzw. die Faszination von Onlinespielen? „Es macht einfach Spaß“, so die Antwort vieler Jugendlicher. Abenteuer sind in ihrer Realität kaum noch zu erleben. Genau das ist es jedoch, was Heranwachsende suchen. In Computerspielen wie „World of Warcraft“ wimmelt es von Elfen und anderen mystischen Gestalten. Fantasie und Kreativität können hier „erlebt“ werden. Beim Besiegen von magischen Ungeheuern sind die Spieler die Helden.

Für Eltern stellt sich jedoch die Frage, wie viel Spielzeit noch normal ist, ohne dass sie befürchten müssen, ihr Kind könne computersüchtig werden.

Insbesondere Internet-Rollenspiele, die in Gruppen zusammen gespielt werden, verleiten die Jugendlichen zum längeren Spielen. „Ich kann die anderen doch jetzt nicht im Stich lassen“, so die Antwort der Spieler, wenn die Eltern zum Aufhören drängen. Erst wenn Eltern sich die Zeit nehmen und ihren Kindern beim Spielen zuschauen, können sie die Spiele bzw. ihre Kinder verstehen. Jugendliche müssen merken, dass sich Eltern für ihre Aktivitäten interessieren, auch wenn es PC-Spiele sind. Durch gemeinsame Erfahrungen können die Argumente des Gesprächspartners besser verstanden und akzeptiert werden.

Dr. te Wildt hat in seiner Sprechstunde Menschen untersucht, die durch die Abhängigkeit vom Internet oder von Computerspielen starken Leidensdruck entwickelt haben und psychiatrischer Unterstützung bedurften. Am Vortragsabend wird te Wildt eventuelle Zusammenhänge von Computerspielsucht und Gewalt, Amoklauf und ADHS erläutern. Wenn eigene Bedürfnisse, wie Essen, Schlafen und Körperpflege im realen Leben total vernachlässigt werden und soziale Kontakte nur noch übers Internet „erlebt“ werden, ist das schon als Sucht zu bezeichnen. Eltern, Erzieher und Lehrer sollten die Symptome einer beginnenden Internetsucht erkennen.

Selbstverständlich muss ein vernünftiger Umgang mit dem PC erlernt werden. Kein berufliches Ziel lässt sich ohne Computerfähigkeiten erreichen. Jedoch ist es der sinnvolle Umgang, den die Heranwachsenden lernen müssen. Der Vortragsabend soll die Teilnehmer für die Internetnutzung unserer Jugendlichen sensibilisieren. Für Lehrer ist er als Fortbildung von der regionalen Lehrerfortbildungsstelle in Wolfsburg anerkannt.

Vorwort

In Kooperation mit dem Gröninger Bad aktion musik e. V. und der Fachhochschule Polizei Sachsen-Anhalt wurde auf Initiative und im Auftrag des Landeskriminalamtes Sachsen-Anhalt das Musikvideo „Ich bin online“ entwickelt.

Ziel des Musikvideos ist es, Schülerinnen und Schüler (ab 10 Jahren) über Cybermobbing (Mobbing über Internet/ Handy) aufzuklären und ihnen die Folgen für Täter und Opfer vor Augen zu führen.

In dem vorliegenden Begleitheft werden Informationen über Cybermobbing gegeben sowie Wege und Ansätze aufgezeigt, wie man sich gegen solche Machenschaften zur Wehr setzen kann.

Musik

Gesang:	Angela Peltner
Text:	Martin Peltner
Arrangement:	Jürgen Schienemann/ Lars Hengmith
Gitarre:	Jürgen Schienemann
Bass:	Martin Peltner

Darsteller

Angela:	Angela Peltner
Band:	Die Gruppe „In my Days“ (Steven Samsel, Charly Schröder, Tino Finke)
Freund:	Dennis Zwickert (In my Days)
Chef:	Steven Henkel
Freundinnen:	Sina-Maria Gallein, Ina Ehrentraut
junger Mann (Bar):	Max Nehrig

Produktionsleitung:	Gregor Schienemann
Regie:	Benjamin Kober
Licht:	Martin Peltner
Assistenz:	Max Nehrig, Carolin Soyke

Vielen Dank an folgende Personen für die Bereitstellung der Locations:

Mario Eckardt/Go Cart Bahn Magdeburg,

Gregor Schienemann/Gröninger Bad Magdeburg,

Jörg Urbach/Urbar Magdeburg,

StevenHenkel/Versicherungsbüro,

Martin Peltner/Wohnung!

Songtext

Ich bin online

Refrain:
Ich bin online 1,2,3
und mein Chef hat mich gefeuert, Sauerei.
Ich bin online, oh mein Gott
ich habe mehr Klicks als Paris Hilton auf' m Pott, auf' m Pott.

Strophe:
Völlig blau aufgewacht, keine Ahnung von letzter Nacht
dunkle Wolken ziehen rauf, im Internet tauchen Fotos auf.
Von mir und meinem Freundeskreis,Frau Bier und Herr Wodka auf Eis.
auf Facebook kursiert das Gerücht, ich habe 'nen fremden Typ geküsst.

Und 100 Kommentare, gehen minütlich rein
verflucht was ich so mag, könnt jetzt mein Verhängnis sein.

Refrain:
Ich bin online 1,2,3
und mein Chef hat mich gefeuert, Sauerei.
Ich bin online, oh mein Gott
ich habe mehr Klicks als Paris Hilton auf' m Pott, auf' m Pott.

Strophe:
Und diese Susi von StudiVZ, hab ich total falsch eingeschätzt
postet 'nen Video von mir auf dem Toilettenrand.
ich habe mich fast nicht mehr erkannt.
lallend sing ich " La, La, La" und meine Hose
sitzt nicht mehr so wie sie war.
was ne dumme Pose.

Ich krieg ne SMS, super mein Freund macht jetzt schon Stress.
Er will mich sofort sehen, doch vorher muss ich kotzen gehen.

Refrain:
Ich bin online 1,2,3
und mein Chef hat mich gefeuert, Sauerei.
Ich bin online, oh mein Gott
ich habe mehr Klicks als Paris Hilton auf' m Pott, auf' m Pott

Strophe:
Morgen ist wieder Samstag
morgen hört es auf.
da gibt´s ne neue Party
und mein Video das fliegt raus.

Ich bin offline 1,2,3
ich schmus mit meinem Freund und ihr seid nicht dabei.

Allgemeine Information zu Cybermobbing

Was ist Cybermobbing?

Cybermobbing weist die gleichen Tatumstände auf wie „klassisches" Mobbing, es bedient sich lediglich (ergänzend) anderer Methoden. Die Täter/-innen nutzen Internet- und Mobiltelefondienste zum Bloßstellen und Schikanieren ihrer Opfer. Hierzu zählen im Internet E-Mails, Online-Communities, Mikrobloggs, Chats (Chatrooms, Instant Messenger), Diskussionsforen, Gästebücher und Boards, Video- und Fotoplattformen, Websites und andere Anwendungen. Mobiltelefone werden genutzt, um die Opfer mit Anrufen, SMS, MMS oder E-Mails zu tyrannisieren. Die Ausstattung der Mobiltelefone mit Foto- und Videokamera, Sprachaufzeichnungsmöglichkeit und Internetzugang gibt jungen Menschen hierzu leicht nutzbare Technologien in die Hand.

Beim Cybermobbing können die Täter/-innen rund um die Uhr aktiv sein, das heißt, ihre Aktivitäten erfordern keinen direkten Kontakt zum Opfer. Täter/-innen finden im Internet zudem ein großes Publikum, tausende Menschen können die Taten verfolgen, sie kommentieren oder unterstützen. Die veröffentlichten Texte, Fotos oder Videos werden von anderen Personen weiterverbreitet und somit weiteren Menschen zugänglich gemacht. Umfang und Auswirkungen der Veröffentlichungen zum Nachteil des Opfers sind somit weder zu steuern noch sind sie überschaubar. Da das Internet nichts vergisst, also selbst gelöschte Inhalte immer wieder auftauchen können, ist es möglich, dass das Opfer selbst nach einer Beendigung des Konfliktes mit dem Täter immer wieder mit den Veröffentlichungen konfrontiert wird.

Cybermobbing ist mittlerweile keine Ausnahmeerscheinung mehr. Insbesondere an Schulen tritt das Problem häufig zu Tage. Das liegt vor allem daran, dass junge Menschen verstärkt über soziale Netzwerke (Wer kennt wen usw.) kommunizieren. Schulklassen oder ganze Schulen sind auf diese Weise miteinander vernetzt. Hänseleien und Beleidigungen finden nicht mehr nur im Klassenzimmer und auf dem Schulhof statt, sondern werden ins Internet verlagert. Dort ist es besonders leicht, andere zum Opfer zu machen – die Täter/-innen wähnen sich sicher in der Anonymität des Netzes.

Begriffsdefinition und das System „Mobbing"

Mobbing ist ein aggressives Verhalten, mit dem ein anderer Mensch absichtlich körperlich oder psychisch geschädigt wird.

Es ist ein Verhalten,

- das sich über einen längeren Zeitraum erstreckt,
- bei dem immer wieder die gleiche Person das Opfer ist,
- bei dem das Opfer sich nicht (mehr) wehrt bzw. wehren kann,
- bei dem der/die Täter/-innen eine Machtsituation ausnutzen.

Die Ursachen für Mobbing sind vielfältig, es kann sich praktisch überall entwickeln. Die Anlässe für Mobbing sind häufig banal. Mitunter genügt es, dass ein späteres Opfer „anders" als die anderen ist. Dies können äußere Merkmale sein (Kleidung, Style, Sozialstatus etc.). Aber auch Verhaltens- oder Arbeitsweisen sowie politische, kulturelle oder religiöse Zugehörigkeiten können einen Anlass für Mobbing geben.

Mobbing ist in allen Altersstufen verbreitet. Schwerpunkte bei jungen Menschen bilden die Klassenstufen sechs bis zehn. An dem Mobbing-Prozess sind jedoch neben Täter/-in und Opfer weitere Personen oder Gruppen beteiligt. Die Täter/-innen erfahren Begleitung und Unterstützung durch „Assistent/-innen", die durch eigene unterstützende Aktivitäten am Mobbing mitwirken. Hinzu kommen „Helfer/-innen" bzw. „Verstärker/-innen", die den Aktivitäten zustimmen und sich durch kommunikative Aktivitäten an der Verstetigung und Ausbreitung des Mobbing-Prozesses beteiligen. Auf der Seite des Opfers stehen „Verteidiger/-innen", die dem Opfer Unterstützung bei der Bewältigung des Problems geben und Hilfe organisieren. Die größte Gruppe bilden jedoch die passiven „Zuschauer/-innen", die zwar Kenntnis von dem Mobbing-Prozess haben, sich aber weder der Opfer- noch der Tätergruppe anschließen. In der pädagogischen Praxis sollte es das Ziel sein, letztgenannte Gruppe zu sensibilisieren und zu aktivieren. Die „schweigende Masse" begünstigt die Verstetigung des Mobbings.

Wie erkennt man Cybermobbing?

Es ist schwer, Fälle von Cybermobbing rechtzeitig zu erkennen. *Oft erfahren Lehrer und Eltern erst spät von dem Vorfall.* Dabei ist ein frühzeitiges Einschreiten sowohl für das Opfer als auch für die Täter wichtig, um die Situation nicht eskalieren zu lassen.

- Eine *Verschlechterung des Klassenklimas* beispielsweise kann Hinweise auf Cybermobbing geben. So genannte Schülermobbing (Smob)-Fragebogen können dabei helfen, das Klassenklima richtig einzuordnen.

- *Ausgrenzungen eines bestimmten Schülers* kommen häufig bei Schulveranstaltungen und Klassenfahrten ans Tageslicht – hier müssen Lehrer ebenfalls reagieren.

- *Der Austausch mit anderen Lehrern* kann dazu beitragen, einen Verdacht zu entkräften oder zu bestärken. Dadurch kann unter Umständen auch ein potenzielles Opfer frühzeitig ausgemacht werden.

- Auch die Einrichtung eines *„anonymen Briefkastens“* kann Cybermobbing aufdecken helfen. Opfer sollten sich hier anonym melden können. Es ist wichtig, dass sofort reagiert wird, wenn ein Fall über den anonymen Briefkasten „angezeigt“ wird.

- Ein Einzelgespräch mit einem möglichen Opfer kann dabei helfen, die Schwere eines Mobbing-Sachverhaltes einzuordnen. Das hilft dabei zu entscheiden, ob die Polizei eingeschaltet werden muss.

Folgen für die Opfer bei Cybermobbing

Die Opfer der Internetattacken können eine Vielzahl an Symptomen aufweisen, die auf Cybermobbing schließen lassen. Die Anzeichen ähneln anderen psychischen Belastungen. Problematisch ist, dass vor allem auch das Privatleben der Opfer von Cybermobbing geprägt ist. Sie sind häufig bedrückt, ungewöhnlich schweigsam oder nervös und angespannt. Viele leiden unter schwerwiegenden psychischen, psychosomatischen und sozialen Folgen wie Schlaf- und Lernstörungen, Schulängste, Depressionen, Selbstverletzungen oder körperlichen Erkrankungen. Die meisten Mädchen und Jungen erzählen weder Eltern noch Lehrkräften/Pädagog/-innen von ihrer Situation.

Weitere Indikatoren, die auf eine Opferwerdung hindeuten können:

- Es wird nach Ausreden für zerstörte oder scheinbar verlorengegangene persönliche Gegenstände gesucht.

- Im Zusammenhang mit dem Schulbesuch treten unerklärliche körperliche Beschwerden auf.

- Das Opfer erhält keine Einladungen beispielsweise zu Kindergeburtstagen oder Partys.

- Das Opfer will nicht mehr mit dem Bus zur Schule fahren oder will häufiger von den Eltern gebracht und abgeholt werden.

- Das Opfer spielt seine eigene Situation vor Erwachsenen herunter.

Straftaten im Zusammenhang mit Cybermobbing

Es gibt keinen speziellen Tatbestand, der Cybermobbing unter Strafe stellt. Gleichwohl können durch Cybermobbing verschiedene Straftatbestände verwirklicht werden: Grundsätzlich sind Kinder unter 14 Jahren strafunmündig.

Beleidigung (§ 185 StGB):
Ob eine strafbare Beleidigung vorliegt, ist abhängig vom Wortlaut sowie dem Gesamtzusammenhang. Auch Fotomontagen oder Gesten wie der „Stinkefinger" können im Gesamtzusammenhang als Beleidigung gesehen werden. Eine Beleidigung wird mit einer Geldstrafe oder einer Freiheitsstrafe bis zu einem Jahr geahndet. Kommt noch eine Tätlichkeit hinzu, steigt die Freiheitsstrafe auf bis zu zwei Jahre.

Verletzung des Rechts am eigenen Bild (§ 22 Kunsturhebergesetz [KUG]):
Jeder Mensch darf entscheiden, ob und welche Bilder von ihm veröffentlicht werden. In Klaras Fall wurden die Bilder ohne ihr Wissen ins Internet gestellt. Damit hat sich der Täter strafbar gemacht. Dieser Verstoß wird mit einer Geldstrafe oder einer Freiheitsstrafe bis zu einem Jahr geahndet.

Weitere Straftatbestände, die beim Cybermobbing erfüllt sein können:
Üble Nachrede (§ 186 StGB), Verleumdung (§ 187 StGB), Nötigung (§ 240 StGB), Bedrohung (§ 241 StGB), Erpressung (§ 253 StGB), Verletzung der Vertraulichkeit des Wortes (§ 201 StGB), Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB), Verletzung des Briefgeheimnisses (§ 202 StGB), Gewaltdarstellungen (§ 131 StGB), Nachstellung (Stalking, § 238 StGB) etc.

Als strafrechtliche Nebenfolgen kommt auf jeden Fall die Einziehung der Tatmittel (Handy, Notebook, Smartphone, PC) in Betracht. Dies gilt auch für Kinder unter 14 Jahre.

Handlungsempfehlungen

Was tun bei Cybermobbing?

Die Schule/Schulleitung muss nach Bekanntwerden eines Falls sofort reagieren.

Folgende Fragen sollten geklärt werden:

Was ist konkret vorgefallen?
Welche Personen sind beteiligt?
Welche Sofortmaßnahmen sind erforderlich?

Mit den Beteiligten reden:
Opfer und Täter sollten getrennt befragt werden. Beziehen Sie dann die Polizei ein, wenn Straftaten für Sie erkennbar sind. Fragen Sie auch bei Ihrer Polizei nach, ob Präventionsbeamte zur Verfügung stehen, die das Phänomen Cybermobbing im Unterricht thematisieren können.

Schutz des Opfers signalisieren:
Stärken Sie das Opfer, indem Sie in der Klasse eindeutig Stellung für das Opfer beziehen.

Eltern einbinden:
Eltern haben oft keine Vorstellung davon, was Cybermobbing ist. Die Schule sollte sie daher informieren und gegebenenfalls den Ernst der Lage deutlich machen.

In der Schule thematisieren:
Cybermobbing darf nicht totgeschwiegen werden. Jeder Fall sollte aufgeklärt werden.

1. Zeigen Sie deutlich, dass Cybermobbing (Gewalt jeder Art) nicht geduldet wird.

2. Bestehen Sie auf eine Entschuldigung der Täter/-innen beim Opfer und regen Sie eine Wiedergutmachung an.

Umgang mit Internet und Handy regeln:
Eindeutige Regelungen zum Umgang mit Handy und Internet in der Schule und im Unterricht sollten in der Schulgemeinschaft festgelegt werden.

Tipps und Infos für Opfer von Cybermobbing zum Weitergeben

- Beleidigende oder sogar bedrohliche E-Mails dürfen nicht toleriert werden. Deshalb: Vertrauen Sie sich Freunden oder Eltern an! Kinder und Jugendliche sollten aber nicht direkt auf solche E-Mails oder SMS antworten, sondern Eltern und andere Vertrauenspersonen einbeziehen.
- Bewahren Sie Beweismaterial auf. Speichern Sie die verbreiteten Bilder und beleidigenden E-Mails und SMS.
- Wenden Sie sich in schwerwiegenden Fällen sofort an die Polizei und erstatten Sie Strafanzeige.
- Bei Schülern sollte auch die Schule informiert werden.
- Bilder und Videos, die ohne Erlaubnis des darin Gezeigten veröffentlicht werden, sollten immer wieder gelöscht werden. Die Löschung kann über den Netzwerkbetreiber vorgenommen werden. Auch so genannte Fake-Profile (die andere im Namen des Betroffenen erstellt haben) können so ebenfalls aus dem Netzwerk entfernt werden.

Hinweis: Je nach Netzwerkbetreiber sind die Voraussetzung für das Löschen von Daten, Bildern oder ganzen Profilen unterschiedlich.

- *Weiterführende Informationen und Internetseiten:*

www.polizei-beratung.de

www.time4teen.de

www.klicksafe.de

www.irights.info

www.saferinternet.at

www.lehrer-online.de

www.jugendschutz.net

www.mobbing.seitenstark.de

www.nummergegenkummer.de

Quelle:

Filmbegleitheft „Netzangriff“
Polizeiliche Kriminalprävention der Länder und des Bundes

Allgemeine Hinweise zur Internetsicherheit

- Das Internet ist kein rechtsfreier Raum. Auch hier gelten Recht und Gesetz.
- Hüten Sie Ihre persönlichen Daten so wie in der realen Welt!
- Das Internet hat ein langes Gedächtnis. Einmal eingestellte Daten sind nur sehr schwer wieder zu entfernen.
- Machen Sie sich bewusst, dass Ihre persönlichen Daten für viele sichtbar sind und von anderen missbraucht werden können!
- Auch Sie hinterlassen mit einer Protokolladresse bei jeder Aktion eine Spur im Internet.
- Niemand hat im Internet etwas zu verschenken, viele Dienste werden durch Werbung und Datennutzung oder -weitergabe finanziert.
- Widersprechen Sie der Nutzung Ihrer Daten zum Zwecke der Werbung, Markt- und Meinungsforschung bei den Unternehmen!
- Beenden Sie jede Internetsitzung (mit Anmeldung) stets über die Abmeldefunktion!

Verhinderung von Vieren, Würmern, Trojanern und unberechtigten Zugriffen

- Installieren und aktualisieren Sie eine Vierenschutzsoftware auf Ihrem Computer und starten Sie regelmäßig einen Suchlauf!
- Aktualisieren Sie regelmäßig Ihr Betriebssystem und Ihren Internetbrowser (z. B. Windows-Update, Windos-Explorer-Update), um Sicherheitslücken zu schließen, über die sonst ungehindert Schadsoftware eindringen könnte! Für eine zeitnahe Auffrischung des Schutzes ist es sinnvoll, automatische Update-Dienste zu nutzen.
- Schränken Sie den Zugriff auf Ihren Computer ein (Firewall, Benutzerkonten)!
- Nutzen Sie Programme, die Sie vor unseriösen Internetseiten warnen!

Passwörter sichern

- Kombinieren Sie Passwörter mit Zahlen, Buchstaben und Sonderzeichen von mindestens acht Stellen!
- Wählen Sie keine Passwörter aus dem Wörterbuch, Namen, Geburtsdaten oder einfache Zahlen- und Buchstabenfolgen!
- Bilden Sie einen einprägsamen Satz und nutzen Sie die Anfangsbuchstaben der Wörter und Satzzeichen als Passwort!
- Speichern Sie die Passworte keinesfalls auf dem Computer!
- Ein regelmäßiges Wechseln des Passwortes erhöht die Sicherheit.
- Verwenden Sie für verschiedene Zugänge keine einheitlichen Passworte!

Einkauf im Netz

- Bevorzugen Sie vertrauenswürdige Internetseiten, die Ihnen bekannt sind oder empfohlen wurden!
- Prüfen Sie die allgemeinen Geschäftsbedingungen und das Impressum Ihnen bekannter Anbieter!
- Achten Sie auf Zertifikate, Gütesiegel und Hinweise im Bewertungsportal, um seriöse Anbieter zu finden!
- Überprüfen Sie bei Online-Auktionen das Profil ihres potentiellen Vertragspartners!
- Beziehen Sie keine Medikamente von unseriösen Anbietern im Internet!

- Nutzen Sie verschlüsselte Verbindungen (auf https:// und Schlosssymbole in der Adresszeile achten) und bevorzugen Sie sichere Bezahlverfahren, wie Bankeinzug oder Rechnung!

- Informieren Sie sich auch über gebührenpflichtige, aber sichere Internetbezahlverfahren (z. B. Paypal, Firstgate)!

Sichere Bankgeschäfte

- Lassen Sie sich von Ihrer Bank zum sicheren Internetverkehr beraten!

- Schützen Sie Ihre Zugangsdaten sowie Transaktionsnummern (Pin und Tan) vor unberechtigtem Zugriff und speichern Sie diese nie auf dem Computer!

- Prüfen Sie die Echtheit Ihrer Bank-Webseite und geben Sie die Internetadresse Ihrer Bank stets von Hand ein!

- Ignorieren Sie E-Mails, die Sie zur Eingabe Ihrer Kontodaten auffordern! Keine Bank würde Sie dazu veranlassen (Gefahr von Phishing = Passwörter abluxen).

- Vereinbaren Sie ein Limit für tägliche Geldbewegungen und sperren Sie Ihren Kontozugang, wenn Ihnen etwas verdächtig vorkommt!

- Verwenden Sie verschlüsselte Verbindungen und aktuelle Schutzsoftware, um Ausspähungen zu verhindern!

Soziale Netzwerke und Kontaktbörsen

- Lesen Sie zum Schutz Ihrer einzustellenden Daten die allgemeinen Geschäftsbedingungen und Bestimmungen zum Datenschutz des Anbieters!

- Nutzen Sie unbedingt die angebotenen Privatisierungseinstellungen!

- Kommunizieren Sie zu Ihrer eigenen Sicherheit ausschließlich unter Pseudonym!

- Veröffentlichen Sie private Informationen, Texte und Bilder sehr zurückhaltend und in keinem Fall reale Anschriften und Erreichbarkeiten!

- Achten Sie bei der Auswahl des Netzwerkes auf seriöse Betreuung und Führung der Online-Gemeinschaft! Beziehen Sie die Erfahrungen Ihnen bekannter Nutzer ein!

- Seien Sie skeptisch gegenüber Kontaktanfragen Ihnen unbekannter Personen!

- Melden Sie aufdringliche Kontakte dem Betreiber des Netzwerkes!

- Seien Sie äußerst misstrauisch, wenn Online-Bekannte Sie um Geld oder andere Leistungen bitten!

Elektronische Post

- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter und öffnen Sie scheinbar ungefährliche Datenanhänge nie ungeprüft! Fragen Sie beim Absender nach, sollten Sie unsicher sein!

- Seien Sie insbesondere sorgsam im Umgang mit eingehenden E-Mails Ihnen unbekannter Absender und öffnen Sie nicht deren Dateianhänge (Gefahr des Einschleusens von Schadprogrammen)!

- Werden Sie bei E-Mails mit Schlagworten, wie „Mahnung“, „Ihre Rechnung“ oder „Inkasso“ in der Betreffzeile misstrauisch, oftmals verbergen sich dahinter Gaunereien!

- Seien Sie ebenso vorsichtig bei Gewinnbenachrichtigungen und Angeboten zum Geldtransfer, oft verraten Sie unseriöse Nachrichten mit einem Betreff, der den Adressaten neugierig machen soll!

Download nach Maß

- Laden Sie Programme oder Dateien nur von Ihnen bekannten und vertrauenswürdigen Seiten auf Ihren Rechner!

- Vertrauen Sie im Zweifel auf Originalsoftware, denn Gratisangebote dubioser Anbieter könnten mit Schadprogrammen infiziert sein!
- Achten Sie bei vermeintlich kostenlosen Diensten auf das „Kleingedruckte“, ein Download kann unter Umständen in einem kostenpflichtigen Vertrag münden (Abo-Falle)!
- Widersprechen Sie unberechtigten Zahlungsaufforderungen und holen Sie sich professionellen Rat!
- Seien Sie besonders aufmerksam, wenn Sie vor dem Download zur Eingabe Ihrer persönlichen Daten aufgefordert werden, dies kann ein Hinweis auf eine Falle sein!
- Prüfen Sie vor dem Download per Suchmaschine die Seriösität des Anbieters!
- Achten Sie beim Herunterladen von Musik, Filmen oder Spielen, insbesondere im Rahmen von Tauschbörsen darauf, dass keine Urheberrechte verletzt werden!

Achtung Abzocke

- Lesen Sie das Kleingedruckte genau! Vermeintlich kostenlose Dienste entpuppen sich beim Lesen der Allgemeinen Geschäftsbedingungen oft als kostenpflichtig. Achten Sie auf versteckte Kostenhinweise!
- Klicken Sie sich nicht unbedarft durch Anmeldeformulare! Durch ein gesetztes oder fehlendes Häkchen könnten Sie ungewollt den Verzicht auf Widerruf erklären.
- Lassen Sie sich nicht mit Sach- oder Geldpreisen zur Eingabe Ihrer persönlichen Daten ködern!
- Prüfen Sie die Angaben im Impressum! Unseriöse Anbieter hinterlegen oft nur die Adresse eine Postfaches, Auslandsadressen oder schalten Telefonnummern mit Bandansage.
- Lassen Sie sich nicht von Internetadressen irreführen, die denen bekannter Anbieter täuschend ähnlich sind!

Hilfe annehmen

- Fragen Sie Bekannte oder Verwandte nach ihren Erfahrungen mit dem Internet und lassen Sie sich bei den ersten Schritten begleiten!
- Nehmen Sie bei Bedarf Beratung und Hilfe Ihrer örtlichen Verbraucherzentrale in Anspruch!
- Erstatten Sie Anzeige bei der Polizei, wenn Sie trotz aller Vorsicht Opfer einer Straftat geworden sind!
- Nutzen Sie einschlägige Fortbildungsangebote Ihrer regionalen Bildungsträger (z. B. Volkshochschule)!

Weitere Informationsquellen:

www.bsi-fuer-buerger.de
www.computerberatung.de
www.internet-guetesiegel.de
www.internet-sicherheit.de
www.safer-shopping.de
www.trustedshops.de
www.verbrauerzentrale.de
www.klicksafe.de
www.verbraucher-sicher-online.de
www.msa-online.de

Quelle:

Broschüre: Senioren im Internet – aber sicher!
Herausgeber: Landesrat für Kriminalitätsvorbeugung Mecklenburg-Vorpommern

Impressum

Herausgeber:
Landeskriminalamt Sachsen-Anhalt
Polizeiliche Kriminalprävention
Lübecker Str. 53 – 63
39124 Magdeburg

Pädagogisch-didaktische Gestaltung:
fjp>media e. V. – Verband junger Medienmacher
Sachsen-Anhalt
Medientreff zone!
Gareisstraße 15
39106 Magdeburg

Video- und DVD-Produktion:
Gröninger Bad aktion musik e. V.
Gröninger Str. 2
39122 Magdeburg

Layout/Herstellung:
Fachhochschule Polizei Sachsen-Anhalt
Medienzentrum
Schmidtmannstraße 86
06449 Aschersleben