Doug Fodeman, Marje Monroe

Passwords, Phishing und private Daten – sicher leben im Internet

Ein Projekthandbuch

TibiaPress

Inhalt

Vorwort

Im Zusammenhang mit Internetsicherheit sollte uns bewusst sein, dass auch im Internet, genau wie im richtigen Leben, nichts kostenlos ist. Im World Wide Web ist die Währung meist nicht das Geld, sondern es sind unsere persönlichen Daten, mit denen wir die (vermeintlich kostenlosen) Dienste bezahlen. Aus diesem Grund muss man sich, genau wie beim normalen Kauf von Produkten, überlegen, wie viel man bereit ist zu zahlen. Jeder sollte deshalb darauf achten, dass er nur in einen Handel einwilligt, bei dem sich Kosten und Nutzen die Waage halten und bei dem er die Gefahren einschätzen kann. Jeder sollte darauf aufpassen, dass er nicht betrogen und abgezockt wird. Im Web ist es so wie im richtigen Leben, nur, dass immer alle zuschauen.

„Passwords, Phishing und private Daten – sicher leben im Internet" ist in erster Linie ein Arbeitsbuch zum Thema Internetsicherheit, das grundlegende Informationen zu Themen wie der richtigen Passwortwahl, zur Online-Privatsphäre, zu Identitätsdiebstahl oder Cyber-Mobbing bietet. Vertieft werden diese Themen durch die zahlreichen Links zu nützlichen Websites, Dokumenten und Onlinequellen, die am Ende eines jeden Kapitels und im Kapitel selbst zu finden sind. Da sich das Internet ständig wandelt, lässt es sich nicht verhindern, dass einige Links in diesem Buch im Lauf der Zeit nicht mehr funktionieren werden. Dafür möchten wir um Verständnis bitten. Wenn Sie einen defekten Link finden, senden Sie uns diesen bitte in einer E-Mail an *info@tibiapress.de*. Es wurde eine Extraseite auf unserer Website *(www.tibiapress.de)* eingerichtet. Diese enthält die im vorliegenden Buch enthaltenen URLs nach Kapiteln geordnet. Der Link dazu lautet *http://bit.ly/e94MGC*. Wir werden uns bemühen, die gemeldeten defekten Links durch neue und zusätzliche Internetadressen zu ergänzen.

Dieses Projekthandbuch ist nicht nur für den klassischen Schulunterricht gedacht, sondern kann genauso in außerschulischer Kinder- und Jugendarbeit sowie in der Erwachsenenbildung eingesetzt werden. Hier können dann die Begriffe „Schüler", „Kinder" und „Jugendliche" durch „Teilnehmer" und „Erwachsene" ersetzt werden.

Pseudonyme

Schülern ist gewöhnlich nicht bewusst, dass das Pseudonym, das sie sich im Internet ausgedacht haben, als Grundlage für schnelle Urteile anderer ausreicht. Dasselbe gilt für eine Schulklasse, die neue Schüler/Klassenkameraden allein nach ihrem Aussehen bewertet.

„Sumpfdudi" konnte nicht verstehen, weshalb er online häufig lächerlich gemacht wurde. „Barbiegirl32" konnte nicht nachvollziehen, dass ihr Pseudonym sie für Pädophile attraktiv machte. Viele Schüler sind zu unbedarft, zu jung oder zu unerfahren: Ihnen ist nicht bewusst, dass ihr Name sich stark auf ihre Onlineerfahrungen auswirken kann.

Selbstverständlich ist den meisten klar: Der erste Eindruck auf einem Foto kann irreführen. Wie wir aussehen und uns kleiden, zeigt nicht immer, ob wir als Freund ehrlich, schlecht oder gut sind. Und dennoch beurteilen uns andere nach unserer Kleidung und nach unserem Aussehen. Alle Menschen – auch Sie und ich – neigen zu vorschnellen Urteilen. Wir achten auf Kleidung, Frisur, Make-up, Schmuck und sogar auf Körperhaltung und das Lächeln und bilden uns danach unsere Meinung über andere. Ist er/sie ein netter Mensch? Kann ich ihm/ihr vertrauen? Könnte ich mich mit ihm/ihr anfreunden?

In Wahrheit wissen wir jedoch erst nach dem Kennenlernen, ob unsere Urteile über andere zutreffen. In Übung 1.1 – Erster Eindruck – werden Schüler gebeten, anhand von Fotos zweier Jungen über ihren ersten Eindruck zu sprechen. Halten sie den einen für einen hervorragenden Schüler, der immer die besten Noten bekommt und stets zum Schülersprecher gewählt wird? Sehen sie im anderen einen in mehreren Fächern schlechten Schüler oder einen, der bei Klausuren häufig schummelt? Hänselt einer der beiden andere? Es soll gezeigt werden, dass niemand eine andere Person anhand ihres Aussehens beurteilen kann.

Auch online urteilen Menschen ständig über andere, häufig jedoch mit noch geringerem Vorwissen. Wenn Schüler zum ersten Mal online mit jemandem in Kontakt kommen, sehen sie lediglich das Pseudonym bzw. den Internetnamen der anderen Person. (Video- oder Audio-Chats nutzen die meisten Schüler für die ersten Kontakte nicht.) Bevor sich Menschen wirklich kennenlernen, beurteilen sie einander auf der Grundlage des Pseudonyms. Daher

sind die Namen sehr wichtig. In Übung 1.2 – Was ist ein Pseudonym? – werden Schüler gebeten, zu diskutieren, weshalb einige Pseudonyme möglicherweise schlecht gewählt sind.

Schüler wollen im Internet natürlich auf sich aufmerksam machen, und deshalb suchen sich selbst jüngere manchmal Namen mit vulgären oder sexuellen Inhalten oder Anspielungen aus.

Bei der Gruppe der älteren Schüler müssen zusätzliche Gesichtspunkte besprochen werden: Diskriminiert das Pseudonym Frauen oder Männer? Ist es rassistisch? Lässt es den Schüler in einem schlechten Licht erscheinen? Eine Vierzehnjährige mit dem Pseudonym „Schnitte" ist sich möglicherweise nicht darüber im Klaren, was ihr aufgrund ihres Namens droht. Sogar wenn sie vielleicht erwartet, dass man mit ihr flirtet, ist sie sehr wahrscheinlich in ihrer persönlichen und emotionalen Entwicklung noch nicht so reif, sexuellen oder belästigenden Bemerkungen zu begegnen, zu denen ein solcher Name einlädt. Dies auf eine Weise anzusprechen, die dem Alter der Kinder und Jugendlichen entspricht, ist wichtig. In Übung 1.3 – Pseudonyme, die zu negativer Aufmerksamkeit führen – werden die Kinder gebeten, Namen zu betrachten, die zu Mobbing führen können.

Einige Pseudonyme geben zu viele Informationen preis. Normalerweise sind Schüler sich nicht bewusst, dass eine kleine Einzelinformation gefährlich werden kann. Die Information, dass ein Mensch einen Karatekurs belegt oder ein Musikinstrument spielt, kann ihn verletzbar machen. Pädophile und andere Personen, die Kinder missbrauchen oder schädigen wollen, sind Meister der Manipulation. Sie kommen in der Regel mit Kindern und Jugendlichen in Kontakt, indem sie für den Aufbau einer Beziehung verwertbare Informationen sammeln. Jedes Detail, das Pädophile kennen, gibt ihnen weitere Mittel an die Hand, ein Kind in ein Gespräch zu verwickeln und die Beziehung weiter auszubauen. Junge Menschen sollten lernen, sehr vorsichtig mit ihren persönlichen Informationen umzugehen. Laut der JIM-Studie 2010 schützen sich nur acht Prozent der befragten Jugendlichen, indem sie nichts Persönliches oder Privates veröffentlichen, und neun Prozent versuchen sich dadurch zu schützen, dass sie keinen Kontakt zu Fremden aufnehmen. Aber immerhin 25 Prozent sind sich bewusst, dass sie sich im Internet am besten schützen, indem Sie nichts bzw. wenig von sich preisgeben. (Quelle: JIM 2010)

Im Internet versuchen Menschen manchmal, andere mithilfe von Tricks dazu zu bringen, Geld auszugeben, verbotene Dinge zu tun oder persönliche Daten preiszugeben, die von Dritten gewinnbringend verwertet werden können. Am einfachsten können Fremde dies tun, indem sie ein Kind neugierig machen oder dessen Interesse wecken, so dass sie es in ein Gespräch verwickeln können. Wenn ein Fremder beim Instant-Messaging, in einem Chatroom oder in einem Onlinespiel zu „AndyKarateKid" sagt „Ich mache auch Karate", wird Andy wahrscheinlich eher mit dem Fremden in Kontakt treten. Bitten Sie in Übung 1.4 – Gibt das Pseudonym Informationen preis? – die Schüler, aus den Pseudonymen so viele Informationen wie möglich über die jeweilige Person abzuleiten.

Tausende von MySpace-Nutzern wurden bereits mit einem Trick dazu gebracht, ihre Benutzerkennungen und Passwörter offenzulegen, indem sie auf einen E-Mail-Link zu einer gefälschten MySpace-Anmeldeseite klickten. (Das Gleiche passierte auch unzähligen Facebook-Nutzern.)

Online gegebene Informationen sind Geld wert. Schüler müssen das begreifen. Eine E-Mail-Adresse kann zum Beispiel an „Spammer" verkauft werden, die anschließend unerwünschte E-Mails senden. In diesen Mails kann Werbung stehen, oder der Empfänger kann dazu verleitet werden, Benutzernamen und Passwörter offenzulegen. Wenn ein „Spammer" weiß, dass eine Person wahrscheinlich ein Musikinstrument spielt (wie in Übung 1.4 bei „Violina"), kann er an diese Person gezielt Junk-E-Mails oder betrügerische Nachrichten senden, die um das Thema Geigespielen kreisen. Je mehr Fremde über Schüler wissen, desto einfacher können sie sie manipulieren. Selbst Erwachsene, die meinen, sie seien mit dem Internet sehr vertraut, können dort getäuscht und manipuliert werden. Eine gute Website zum Thema Werbung ist *http://www.mediasmart.de/wissen.html.* Hier gibt es für Kinder und Erwachsene Informationen rund um das Thema Werbung. (Mehr zum Thema Werbung gibt es in Kapitel 9.)

Am besten sollten Pseudonyme gewählt werden, die möglichst wenige Informationen enthalten und am wenigsten provokativ sind. In Übung 1.5 – Gut und schlecht gewählte Pseudonyme – finden Sie eine Liste mit Pseudonymen. Bitten Sie die Kinder, darüber zu sprechen, welche gut und welche schlecht sind. (Hinweis: In Kapitel 3 Seite 63 wird behandelt, weshalb Schüler in Pseudonymen die Zeichen 1 i l und o O 0 vermeiden sollten.) Bitten Sie in Übung 1.6 – Pseudonyme geschickt auswählen – die Schüler, Pseudonyme zu erstellen, und besprechen Sie anschließend, ob sie gut oder schlecht sind. Die Kinder werden überrascht sein, was andere in ihren Namen erkennen.

Passwörter

Für viele verschiedene Zwecke sind Online-Passwörter nötig. Wir verwenden sie für E-Mails, Instant-Messaging, Blogs, Spiele-Websites, Soziale Netzwerkseiten und Benutzerkonten zum Austausch von Fotos sowie für I-Tunes und andere Shopping-Websites. Leider sind die Passwörter der meisten Menschen nicht besonders sicher und können mühelos „geknackt" werden. Die am häufigsten verwendeten Passwörter sind so einfach, dass sie mit sehr geringem Aufwand erraten werden können. Können Ihre Schüler erraten, welche Passwörter am häufigsten verwendet werden? Es sind folgende:

- Namen von Fußball-, Basketball- und Handballmannschaften
- Geburtstage von Familienmitgliedern
- Die Jahreszahl eines bestimmten Sportereignisses, zum Beispiel das Jahr des Fußballweltmeistertitels
- Das Wort „Passwort" oder „Kennwort" oder eine Variante wie „Passwort1" oder „Kennwort1"
- Die Ziffernfolge „123456" oder die Variante mit der Kombination aus Buchstaben und Ziffern wie „abc123" oder „123abc"
- Der Name eines Familienmitglieds, eines Haustiers, einer Lieblingsfigur aus dem Fernsehen, eines Prominenten oder einer Musikgruppe.

Es gibt Softwareprogramme, mit denen in Onlinebenutzerkonten eingebrochen werden kann. Diese Programme können alle Wörter in Wörterbüchern ausprobieren, um so in ein Konto einzubrechen. Sogar rückwärts buchstabierte Wörter können sie suchen. Einige durchlaufen häufige Wortkombinationen oder Wörter mit angehängten Ziffern wie „Schule222". Diese Programme testen in wenigen Minuten Millionen von Passwörtern.

Schüler können mit dem Quiz in Übung 1.7 – Passwort-Quiz – herausfinden, mit welcher Wahrscheinlichkeit ihre eigenen Passwörter und die ihrer Familienmitglieder erraten werden können. Die Ergebnisse der Übung können in der Klasse besprochen werden. So erhöht sich die Wahrscheinlichkeit, dass die Kinder der Meinung sind, dass sie neue Passwörter erstellen sollten.

Ihre Schüler können einige einfache Richtlinien befolgen, um ein sehr sicheres Passwort zu erstellen, das schwer zu ermitteln ist, das sie sich aber trotzdem noch gut merken können.

Abbildung 1.1 Ein einfach zu erratendes Passwort.
(Nachdruck mit Genehmigung des Künstlers David Saunders.)

Hier einige nützliche Hinweise, die Sie an die Kinder weitergeben können:

- Verwende immer eine Kombination aus Buchstaben und Ziffern.
- Kombiniere Groß- und Kleinbuchstaben miteinander. Bei den meisten Passwörtern muss die Groß-/Kleinschreibung beachtet werden.
- Verwende andere Zeichen als Buchstaben und Ziffern, zum Beispiel = ! $ #. (Einige Websites lassen keine Interpunktionszeichen zu. Du musst also ausprobieren, welche Interpunktions- und Sonderzeichen zulässig sind).