MINISTERUL EDUCAȚIEI NAȚIONALE

Daniel Popa

INFORMATIK UND IKT

LEHRBUCH FÜR DIE VI. KLASSE

EDITURA DIDACTICĂ ȘI PEDAGOGICĂ S.A.

Inhaltsverzeichnis

2. Das Internet

Persönlicher Datenschutz im Internet

Erinnere dich!

1. **Arbeitet paarweise.** Besprich mit einem Kollegen die Gefahren, die es bein Surfen im Internet gibt. Macht zusammen eine Liste und und findet eine Lösung für jede.

Entdecke!

2. Suche im Internet Informationen über „die Online-Sicherheit für Kinder". Lies 2-3 Artikel von der ersten Seite der Suchmaschine und fasse die gemeinsamen Ideen zusammen. Lies den Artikel von der Adresse: http://www.sigur.info/siguranta-online/copii-pe-internet/copii.html. Was für andere Adressen hast du gefunden?

Wichtig

Das Internet ist ein öffentlicher Ort, zu dem jeder Zugang hat. Wenn eine Person Informationen über sich postet (Bilder, persönliche Daten usw.), ist es wie wenn sie ein Werbeplakat in der Mitte der Stadt hat, auf dem sie diese Informationen zeigt. Jeder hat Zugang zu den veröffentlichten Informationen und kann sie benützen, wie er will.

Wenn eine Person, direkt oder indirekt, anhand einiger Informationen oder Daten identifiziert werden kann, dann können diese **persönliche Daten** genannt werden.

Die Daten können folgende sein:

- der Person: Name, Vorname, PIN, Bild (Foto), DNA, Fingerabdrücke;
- über die Person: Sex, Rasse, Alter;
- in Verbindung mit der Person: Heimatadresse, Beruf.

Beispiel: In der Aussage „Ein Schüler aus der Stadt Bukarest …" findet man anonyme Daten, weil man die Person nicht identifizieren kann. Die Aussage „Der Schüler Totescu Kalin, aus der Schule Nr. 7 aus Bukarest ...", enthält genügend (persönliche) Daten, um die Person zu identifizieren.

Die virtuelle Identität ist die Darstellung einer Person im virtuellen Raum. Gewöhnlich ist es ein von einem Passwort geschütztes Konto in einem sozialen Netzwerk, in einem Videospiel oder einem Kommunikationssystem im Internet.

Übe!

3. Führe folgende Internetrecherche durch: „veränderte Bilder", „Bean Gladiator". Zwischen den erhaltenen Resultaten, hast du auch das nebenstehende Bild gefunden, dass kein echtes Bild ist. Von wo hat die Veränderung des Bildes begonnen? Warum glaubst du, dass es verändert wurde? Wie würdest du vorgehen, wenn du ein von dir verändertes Bild finden würdest?

4. Suche im Internet Informationen über dich. Was für Daten hast du gefunden? Suche Informationen über **eine berühmte Persönlichkeit** oder eine sehr bekannte Person in Rumänien. Was für persönliche Information **hast du über diese gefunden?**

2. Das Internet

Persönlicher Datenschutz im Internet

Erinnere dich!

1. **Arbeitet paarweise.** Besprich mit einem Kollegen die Gefahren, die es bein Surfen im Internet gibt. Macht zusammen eine Liste und und findet eine Lösung für jede.

Entdecke!

2. Suche im Internet Informationen über „die Online-Sicherheit für Kinder". Lies 2-3 Artikel von der ersten Seite der Suchmaschine und fasse die gemeinsamen Ideen zusammen. Lies den Artikel von der Adresse: http://www.sigur.info/siguranta-online/copii-pe-internet/copii.html. Was für andere Adressen hast du gefunden?

Wichtig

Das Internet ist ein öffentlicher Ort, zu dem jeder Zugang hat. Wenn eine Person Informationen über sich postet (Bilder, persönliche Daten usw.), ist es wie wenn sie ein Werbeplakat in der Mitte der Stadt hat, auf dem sie diese Informationen zeigt. Jeder hat Zugang zu den veröffentlichten Informationen und kann sie benützen, wie er will.

Wenn eine Person, direkt oder indirekt, anhand einiger Informationen oder Daten identifiziert werden kann, dann können diese **persönliche Daten** genannt werden.

Die Daten können folgende sein:

- der Person: Name, Vorname, PIN, Bild (Foto), DNA, Fingerabdrücke;
- über die Person: Sex, Rasse, Alter;
- in Verbindung mit der Person: Heimatadresse, Beruf.

Beispiel: In der Aussage „Ein Schüler aus der Stadt Bukarest …" findet man anonyme Daten, weil man die Person nicht identifizieren kann. Die Aussage „Der Schüler Totescu Kalin, aus der Schule Nr. 7 aus Bukarest ...", enthält genügend (persönliche) Daten, um die Person zu identifizieren.

Die virtuelle Identität ist die Darstellung einer Person im virtuellen Raum. Gewöhnlich ist es ein von einem Passwort geschütztes Konto in einem sozialen Netzwerk, in einem Videospiel oder einem Kommunikationssystem im Internet.

Übe!

3. Führe folgende Internetrecherche durch: „veränderte Bilder", „Bean Gladiator". Zwischen den erhaltenen Resultaten, hast du auch das nebenstehende Bild gefunden, dass kein echtes Bild ist. Von wo hat die Veränderung des Bildes begonnen? Warum glaubst du, dass es verändert wurde? Wie würdest du vorgehen, wenn du ein von dir verändertes Bild finden würdest?

4. Suche im Internet Informationen über dich. Was für Daten hast du gefunden? Suche Informationen über eine berühmte Persönlichkeit oder eine sehr bekannte Person in Rumänien. Was für persönliche Information hast du über diese gefunden?

Erinnere dich!

5. Welches sind die Regeln, die du einhalten musst, damit du sicher im Internet bist?

Entdecke!

6. Suche im Internet Informationen über „Identitätsdiebstahl im Internet". Beschreibe in zwei oder drei Sätzen, was Identitätsdiebstahl bedeutet. Warum würde jemand die Identität eines anderen stehlen?

Wichtig

Identitätsdiebstahl im Internet ist ein Betrug, durch den eine Person sich die persönlichen Daten einer anderen Person aneignet, weil sie Geld stehlen will oder andere Vorteile haben will.

Methoden für den Identitätsdiebstahl im Internet:

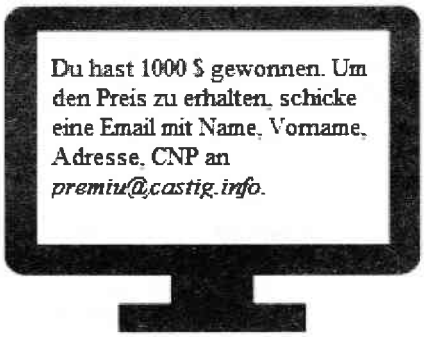
- Identitätsdiebstahl durch E-Mail oder spezialisierte Webseiten (phishing): man verlangt persönliche Daten, damit man eine Belohnung bekommt.
- Anforderung von Informationen beim Surfen im Internet: „nötige" Daten um ein Konto zu erstellen.
- Durch soziale Netzwerke (öffentlich verfügbare Informationen): auf ihnen gepostete Bilder, Arbeitsplatz, Adresse, Telefonnummer usw.
- Anwendung von spezialisierter Software: Programme die das Drücken der Tasten registrieren.

Wie kannst du dich vor dem Identitätsdiebstahl im Internet schützen:

- Veröffentliche auf den sozialen Netzwerken keine Daten über dich: (Geburtsdatum, Telefonnummer usw.).
- Antworte nicht auf E-Mails, die dir persönliche Daten gegen Belohnung fordern.
- Wenn du dir ein Konto auf einer Webseite erstellst musst, dann fülle nur die minimal nötigen Daten aus.
- Wenn man dir persönliche Informationen auf einer Webseite verlangt und du weißt nicht was du machen sollst, dann frage deine Eltern oder einen Erwachsenen in dem du Vertrauen hast, ob du diese Informationen liefern musst.
- Versichere dich, dass du auf dem Computer Sicherheitsmaßnahmen installiert hast.
- Wähle komplizierte Passwörter für dein Konto und benütze nicht dasselbe Passwort für mehrere Konten.
- Wenn du öffentliche Computer benützen must, damit du den Identitätsdiebstahl vermeidest, starte den Computer erneut, starte den Browser im *Incognito Modus* und am Ende starte wieder den Computer.

Übe!

7. Gruppenarbeit. Zusammen mit 3 Kollegen suche Informationen über den Identitätsdiebstahl im Internet. Jeder von euch wählt eine für den Identitätsdiebstahl benützte Methode und die entsprechenden Sicherheitsmaßnahmen. Die gefundenen Informationen benützend, erstellt eine Liste mit den am meisten benützten Methoden für die beiden Kategorien. Für jede Liste ordnet die erhaltenen Resultate, anhand von den meisten gefundenen Adressen in der Suchmaschine.



8. Lies die Nachricht aus dem nebenstehenden Bild.

a) Wie würdest du vorgehen, wenn du so eine Nachricht bekommen würdest? Warum?

b) Was für eine Methode für den Identitätsdiebstahl hast du in dieser Nachricht erkannt?

9. Suche im Internet und finde „wieso brauchen wir Internetsicherheit". Wenn sich zwischen deinen Webseiten auch folgende befinden: sri.ro, bitdefender.ro, nume.blogspot.ro, in welche von diesen würdest du Vertrauen haben? Warum?

10. Gruppenarbeit. Zusammen mit 4 Kollegen besprecht, wie ihr in der V. Klasse gelernt habt, dass ihr euch sichere Passwörter finden könnt. Sucht im Internet Regeln für das Erstellen und Benützen eines sicheren Passwortes. Lest einige Artikel über dieses Thema und für jede der untenstehenden Regeln, zählt wie viele Male sie erscheint. Was für andere Regeln habt ihr noch gefunden?

a) Das Passwort muss lang sein, mindestens 8 Zeichen.
b) Das Passwort muss Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen beinhalten.
c) Benützt keine Wörter aus dem Wörterbuch im Passwort.
d) Benützt nicht dasselbe Passwort für mehrere Konten.
e) Wechsele regelmäßig das Passwort der wichtigen Konten.

11. Welche der untenstehenden Passwörter findest du sicher? Warum?

a) parola1;
b) anaaremere;
c) 4n4_aR3_m3r3;
d) AoCpApRc$3.

12. Suche im Internet Informationen über die ungeeignetsten Passwörter. Ist eines deiner Passwörter ähnlich mit diesen?

13. Suche im Internet Informationen über wie viel deine persönlichen Daten wert sind. Eine Suche in englischer Sprache würde mehrere Informationen liefern, als eine Suche in deutscher Sprache.

Informiere dich!

- Eine Person hat das Recht:

a) den Namen des Bearbeiters zu kennen, den Zweck für den die Daten bearbeitet werden und die Firma/Person zu der die Daten, die Informationen geschickt werden;

b) in einer verständlichen Form eine Kopie der persönlichen Daten zu erhalten und das Beseitigen, Blockieren oder Löschen der Daten anzufordern, wenn diese unvollständig, ungenau oder durch Mittel, die das Gesetz nicht respektieren, erhalten wurden;

c) sich zu weigern, die persönlichen Daten bearbeiten zu lassen;

d) Anspruch auf die Vertraulichkeit der on-line Kommunikation zu haben;

e) informiert zu sein, ob die persönlichen Daten, die von einem Bearbeiter/einer Firma aufbewahrt werden, verloren oder gestohlen wurden.

- Wenn du dir ein E-Mail Konto erstellst oder auf einer Webseite die Zustimmung, für das Bearbeiten der persönlichen Daten geben musst. In den Geschäftsbedingungen wirst du über alles informiert, was die Firma mit deinen persönlichen Daten macht, ebenso was für Rechte und Pflichten du hast.

Wusstest du, dass ...?

❖ Du kannst Passwörter bilden aus einem Satz oder aus zusammengesetzten Sätzen. Zum Beispiel: Aus dem Satz: „Ana are 5 mere si 7 pere.", erhält man das Passwort **Aa_5ms_7p**, indem man den ersten Buchstaben jeden Wortes benützt und indem man das Symbol _ vor die Ziffern tut. Du kannst dir die eigenen Regeln für das Bilden des Passwortes, wenn man von diesem Beispiel ausgeht, finden.

❖ Die Firmen die persönliche Daten sammeln oder bearbeiten, müssen die Kunden informieren, wenn sie persönliche Daten, die sie betreffen, verwenden.

Sicherheitsmaßnahmen im Internet. Benützen der Sicherheitslösungen

Erinnere dich!

1. **Arbeitet paarweise.** Besprich mit einem Kollegen die Regeln, die man für die Sicherheit der virtuellen Daten einhalten muss. An welche Sicherheitsmaßnahmen erinnert ihr euch aus der V. Klasse?

Entdecke!

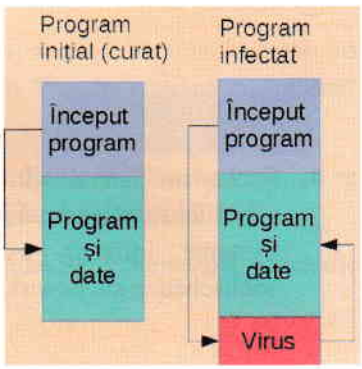
2. **Gruppenarbeit.** Zusammen mit 4 Kollegen erstelle eine Liste mit Typen von Programmen, die dem Computer schaden können. Schreibt vor jedes Programm, was ihr darüber wisst: Was es bewirkt, wie es funktioniert usw.
3. Suche im Internet Informationen über Malware (Schadsoftware). Vergleiche, was du gefunden hast, mit der Liste von der vorigen Übung.

Wichtig

Das Wort **Malware**, erhalten durch das Vereinigen der Wörter *malicious* und *software*, wird benützt um eine Software zu identifizieren, die konzipiert ist, um sich zu infiltrieren und einem Computersystem zu schaden.

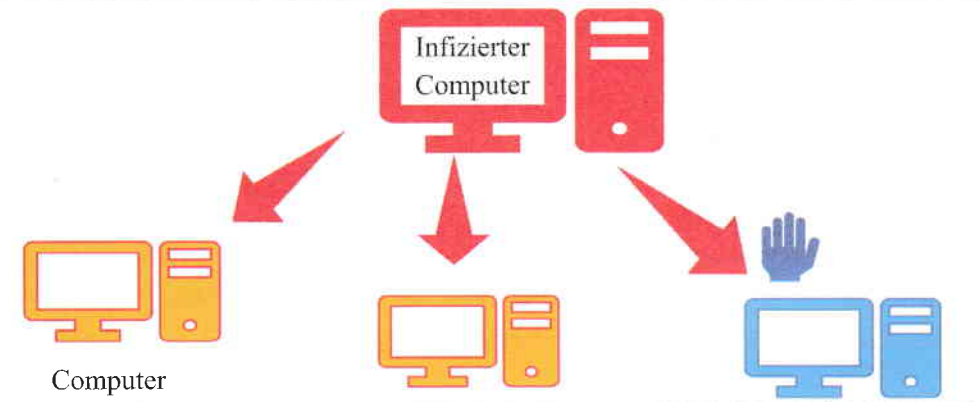
Beispiele für Malware-Programme: Viren, Würmer, Trojaner, Spyware, Adware und andere Schadprogramme.

a) Der Virus, wahrscheinlich eine der bekanntesten Schadsoftware, ist ein kurzes Programm, dass sich an ein anderes Programm anhängt.

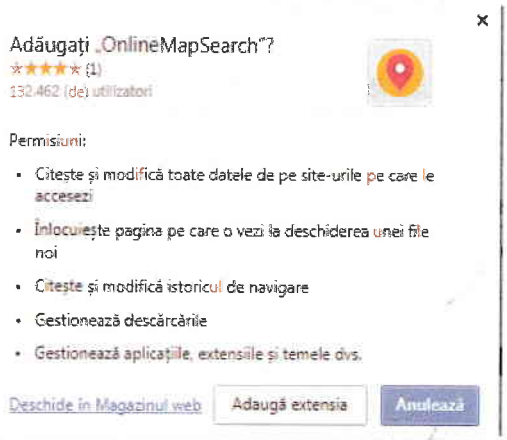


Wie funktioniert er? Bei dem Starten des Programms, startet zuerst der Virus, der sich im Computerspeicher installiert, nachher startet der Virus das eigentliche Programm. Einmal im Arbeitsspeicher, sucht der Virus andere Dateien die nicht infiziert wurden, damit er sie infiziert.

b) Der Wurm ist ein Programm, das sich vermehren kann, ohne die direkte Aktion des Benutzers, indem es sich alleine im Netzwerk auf Datenträger (Memory Stick, externe Festplatten usw.) kopiert.



c) Der Trojaner ist ein Programm, dass eine versteckte Funktionalität hat, die den Fernzugang auf den Computer, auf dem die Anwendung läuft, ermöglicht. Ein Trojaner kann sich in dem Betriebssystem verstecken oder in einem Programm, dass aus dem Internet heruntergeladen wurde. **Achtung!** Das Vorhandensein eines Antivirusprogramms sichert nicht, dass die Trojaner-Anwendung ihren Zweck nicht erreicht.



d) Spyware ist ein Programm, dass jemandem berichtet (gewöhnlich dem Programmentwickler), was du machst, was für Webseiten du besuchst, was du auf einer Webseite eintippst (Passwörter, Bankkonto, usw.), welches dein Verhalten im Internet ist. Ein Großteil der Toolbars (Werkzeugleisten, Schaltflächen im Browser), die verschiedene Dienste im Internet anbieten, haben Spyware-Rolle. Ein Spyware-Beispiel ist rechts.

e) Adware ist eine Spyware-Variante, die nur Werbung auf deinen Computer herunterlädt.

f) Ransomware ist ein Malware Typ, der den Zugang des *Opfers* zu einigen Dateien oder sogar zu dem eigenen Computer sperrt und eine Belohnung dafür verlangt. Sehr oft verschlüsselt das Programm die Daten im Computer. Gegen eine Geldsumme liefert der Programmersteller den Schlüssel für das Entschlüsseln der Daten.

Übe!

4. Suche im Internet Informationen über die schädlichsten Viren. Finde heraus, wie viele Systeme infiziert wurden und was für Sachschäden sie bewirkt haben.

Entdecke!

5. **Gruppenarbeit.** Zusammen mit 3 Kollegen suche im Internet Informationen über den besten Antivirus. Wähle mehrere Quellen und analysiere sie. Bestimme den Durchschnittspreis für eine Sicherheitssuite. Was ist teurer: ein Antivirus zu kaufen oder die Schäden von Malware wiederherzustellen? Warum?

Wichtig

Ein Antivirusprogramm hat die Rolle, Malware zu „jagen" und den Computer davor zu schützen. Wegen den vielen Drohungen, ist ein einfaches Antivirusprogramm nicht mehr ausreichend, sondern es ist eine Suite von Sicherheitsprogrammen nötig.

Dieses sind einige der Unternehmen, die Antivirus-Programme entwickeln.

McAfee Norton WEBROOT Bitdefender KASPERSKY avast EMSISOFT eset F-Secure TREND MICRO

Eine vollständige Sicherheitslösung muss Folgendes anbieten:

a) **Scannen der Dateien auf Anfrage** – prüfen der gewünschten Dateien, damit bestimmt wird, ob diese mit Malware infiziert sind oder nicht.

b) **Scannen der Dateien beim Zugang** – wenn eine Datei geöffnet wird, dann analysiert die Sicherheitslösung vor dem Öffnen, ob die Datei gefährlich ist oder nicht.

c) **Die Analyse der besuchten Webseiten** – die Sicherheitslösung verfolgt, was für Webseiten besucht werden und blockiert den Zugang zu den gefährlichen Webseiten oder warnt dich, dass du eine Webseite besuchst, die deinem Computer (die Webseite ist bekannt, dass sie gefährliche Software liefert) oder dir schaden könnte (Phishing-Seite).

d) **Verhaltensschutz** – die Sicherheitsanwendung prüft für jede im Computer installierte Anwendung, ob sie eine den Malware-Programmen ähnliche Wirkung hat.

e) **Scannen der Software-Schwachstellen** – die Sicherheitslösung prüft, ob das Betriebssystem und die installierten Anwendungen keine Schwachstellen haben.

Übe!

6. Gruppenarbeit. Zusammen mit 3 Kollegen suche im Internet Informationen über die wichtigsten Sicherheitssuiten und fülle eine Tabelle für jede Anwendung aus, ob diese vollständige Sicherheitsmaßnahmen anbietet oder nicht.

7. Arbeitet paarweise. Mit einem Kollegen wähle eine Sicherheitssuite aus, die sowohl gratis als auch kostenpflichtige Lösungen anbietet. Vergleicht die beiden Lösungen. Welche würdest du wählen? Aber dein Kollege? Warum?

8. Suche im Internet „gefälschtes Antivirus-Programm". Worüber ist die Rede? Wie funktioniert so ein Programm? Wie kann man sich vor einem gefälschten Antivirus-Programm schützen?

9. Benütze deine bevorzugte Suchmaschine, um zu bestimmen, welche Sicherheitssuite gegen die Anwendungen vom Typ Ransomware schützt.

Wusstest du, dass...?

- *Creeper* war der erste Virus, der im Jahr 1971 von Bob Thomas geschrieben wurde. Der Virus hat sich vermehrt und hat die Nachricht "I'm the creeper: catch me if you can" (*Ich bin der Bösewicht, fang mich, wenn du kannst*) angeschrieben. Für seine „Jagd" hat man ein anderes Programm, genannt *Reaper* (der Mäher), geschrieben.
- Die Programme vom Typ Malware können als Waffen benützt werden. Stuxnet ist der Name einer Malware, von der man glaubt, dass sie geschrieben wurde, um das Nuklearprogramm des Irans zu beeinflussen. Stuxnet infiltrierte sich auf einen Computer durch einen infizierten USB Memorystick und verbreitete sich auf weitere Memorysticks, die in diesen Computer eingeführt wurden. Stuxnet bewirkte, dass Zentrifugen, die für die Anreicherung des Urans verwendet wurden, sich mit großer Geschwindigkeit gedreht haben, was zu ihrer Zerstörung führte.