Safe and Sound in the Internet

6.59

Vorüberlegungen

Kompetenzen und Unterrichtsinhalte:

- *Die Schülerinnen und Schüler sollen ein Bewusstsein für die Notwendigkeit von Computersicherheit bekommen.*
- *Sie wissen um die wichtigsten Maßnahmen und Vorkehrungen für die eigene IT-Sicherheit.*
- *Sie lernen die Wichtigkeit des Datenschutzes und des Schutzes der digitalen Privatsphäre kennen. Insbesondere bekommen sie ein Bewusstsein dafür, welche Gefahren bei der Nutzung sozialer Netzwerke bestehen können.*
- *Sie erfahren mehr über die Komplexität und die Gefahren der "allgemeinen Geschäftsbedingungen" von sozialen Netzwerken.*
- *Sie lernen, die englischsprachigen Geschäftsbedingungen in deutscher Sprache zusammenzufassen.*

Anmerkungen zum Thema:

IT-Sicherheit ist ein Thema, das **nicht allein auf den EDV-Unterricht** in der Oberstufe reduziert werden darf, da es sich mittlerweile um ein grundlegendes Thema handelt, das in der Selbstkompetenz eines jeden Schülers anzusiedeln ist.

Angesichts der allgegenwärtigen und umfassenden **Nutzung der elektronischen Medien in Schule und Freizeit** ist es wichtig, den Schülerinnen und Schülern diese Thematik auf mehreren Wegen nahezubringen. Der Vorteil einer Verknüpfung mit dem Englischunterricht besteht darin, dass die entsprechende **Fachterminologie** (z.B. Firewall) ohnehin dem englischen Sprachraum entspringt und damit im originären Kontext vermittelt werden kann.

Die Thematik erfordert von Lehrkräften **kein** vertieftes IT-Wissen; das "Know-how" und "Know-why" wird in den Texten und Materialien vermittelt.

Im Fokus steht neben den Fachinhalten vor allem der **fremdsprachige Wortschatz**, der hier fachterminologisch angereichert wird, und dessen **Erwerb**. Da die Schülerinnen und Schüler mit diesem Feld stets (ob beruflich oder privat) zu tun haben werden, ist es legitim, diese Fachterminologie auch einzufordern.

Literatur und Internet zur Vorbereitung:

https://www.verbraucher-sicher-online.de
(eine deutschsprachige Webseite über alle Fragen der Computersicherheit, z.B. sicheres Surfen, soziale Netzwerke, Online-Banking u.a.m.)

http://www.safekids.com/kids-rules-for-online-safety/
(in der Form "I will (not) …" gehaltene Liste von Tipps für Kinder zur Sicherheit beim Umgang mit dem Computer)

http://www.onlinesafety.tv/
(Webseite mit vielfältigen Beiträgen zur Online-Sicherheit)

6.59 Safe and Sound in the Internet

Vorüberlegungen

Die einzelnen Unterrichtsschritte im Überblick:

1. Schritt: Knowledge of Computer Safety
2. Schritt: How to Use the Internet in a Secure Way?
3. Schritt: Personal Data Protection in the Internet
4. Schritt: Facebook – Terms and Conditions
5. Schritt: Identity Theft in the Internet

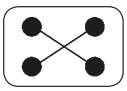
Autor: Diplom-Handelslehrer Clemens Kaesler, M.A., Studiendirektor, geb. 1975, studierte Wirtschaftspädagogik, Betriebswirtschaftslehre und Anglistik an der Universität Mannheim. Derzeit leitet er die höhere Berufsfachschule Sozialassistenz sowie die Fachschule für Organisation und Führung an der Berufsbildenden Schule Ludwigshafen. Daneben ist er als Autor für Unterrichtsmaterialien aktiv und veröffentlicht Aufsätze zum Thema Schulmanagement.

Zum Thema IT bietet Ihnen die *Ideenbörse Englisch Sekundarstufe II* immer wieder Beiträge, die wichtiges Wissen für Ihre Schülerinnen und Schüler bereithalten, zum Beispiel die Unterrichtseinheiten *5.61 Bullying* (aus Ausgabe 62 dieser Reihe) oder *6.51 Online Addiction* (aus Ausgabe 61).

Diese und viele weitere Einheiten finden Sie auch in unserer Online-Datenbank: *www.edidact.de*.

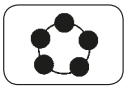
1. Schritt: Knowledge of Computer Safety

Am Beginn der Beschäftigung mit dem Thema "Safe and Sound in the Internet" steht ein *Bildeinstieg* (**Texte und Materialien M 1**$_{(1)}$), der zur Thematik hinführt. Die Schüler sollen Sicherheitsfragen rund um den Computer mit diesen Bildern *assoziieren* und *verbalisieren*.

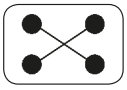


Eine gute Einstiegsmethode besteht darin, die Schüler zunächst in *Partnerarbeit* ihre Gedanken aufschreiben und dann im *Plenum* vortragen zu lassen. Gerade für leistungsschwächere Schüler birgt dieser Einstieg das Potenzial, dass jeder Schüler etwas verbalisieren kann und nicht die schnelleren Schüler diese Lerngelegenheit vorwegnehmen.

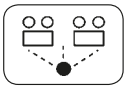
2. Schritt: How to Use the Internet in a Secure Way?



Noch bevor der Text *"Eight Ways to Keep Your Computer Safe"* von **Texte und Materialien M 1**$_{(2–5)}$ gelesen wird, sollen die Schüler im *Unterrichtsgespräch* berichten, mit welchen Maßnahmen sie ihre privaten Computer schützen (**Aufgabe 1**).



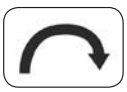
Parallel zum Lesen des Textes erstellen sie dann in *Partnerarbeit* eine Mindmap, die alle acht Bereiche der Computersicherheit veranschaulicht (**Aufgabe 2a**). Der **Vorteil gegenüber der klassischen Textarbeit** besteht darin, dass das Fachwissen sofort in eine Struktur überführt wird und die Schülerinnen und Schüler aktiv mit *Fachterminologie* umgehen müssen.



Im Anschluss daran sollen die Ergebnisse der *Partnerarbeit* in der Klasse *präsentiert* werden (**Aufgabe 2b**). Hierfür ist, wenn vorhanden, der Einsatz einer digitalen Dokumentenkamera nützlich.

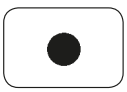
Eine sinnvolle **Verknüpfung mit dem IT-Unterricht** besteht darin, die Mindmap mithilfe einer frei verfügbaren **Freeware** (z.B. **FreeMind**) am PC zu erstellen. Dies ist **alternativ** auch als *Hausaufgabe* denkbar.

Die folgenden Fragen (**Aufgabe 3**) dienen der *Selbsteinschätzung* (*self-evaluation*), d.h. die Schüler können die Mindmap anschließend zur *Überprüfung ihres erworbenen Fachwissens* verwenden. Dabei sollte der Text verdeckt sein.

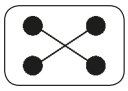


Als *qualitative Differenzierungsmethode* sollen leistungsstärkere Schüler die Fragen ohne Texthilfe beantworten, während die leistungsschwächeren Schüler den Text zu Hilfe nehmen dürfen.

Der Text *"The Dos and Don'ts of Using the Internet"* von **Texte und Materialien M 2**$_{(1)}$ nimmt nicht nur die technische Sicherheitsperspektive, sondern auch den behavioristischen Sicherheitsaspekt in Bezug auf das persönliche Nutzungsverhalten der User im Internet in den Fokus. Er ist sprachlich für Oberstufenschüler sehr einfach zu lesen (Alltagssprache) und dient deshalb als gutes **Sprachvorbild für gesprochenes Englisch**.



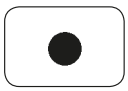
Aus diesem Grund sollen die Schülerinnen und Schüler auch direkt aus diesem Text einen *Kurzvortrag* ableiten (**Aufgabe 1**). Um alle Lerner zu involvieren, ist hier eine *Einzelarbeit* als Sozialform anzuraten.



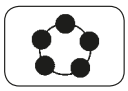
Anschließend sollen die Schüler in *Gruppenarbeit* ein *Poster* gestalten (**Aufgabe 2**), das möglichst kreativ die Ratschläge des Textes visualisiert.

Aufgabe 3: Alternativ zu Aufgabe 2 (oder zur Ergänzung) soll das *cheat-sheet* von **Texte und Materialien M 2$_{(2)}$** die Thematik abrunden. Hier räumt die Lehrkraft den Schülerinnen und Schülern ein, auch noch ergänzendes, eigenes Fachwissen einzubringen. Ziel ist es, eine übersichtliche *Tabelle* zu erhalten, die alle wichtigen Aspekte der Online-Sicherheit (auch in Bezug auf den Datenschutz) darstellt.

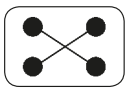
Lösungsvorschläge zu Aufgabe 3 werden in **Texte und Materialien M 2$_{(3)}$** mitgegeben.



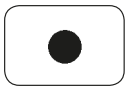
Im Text *"How Malware Works"* von **Texte und Materialien M 3$_{(1+2)}$** wird die Malware-Problematik fachspezifisch thematisiert. Hierzu eignet sich die klassische *Textarbeit*. Die Schülerinnen und Schüler lesen den Text zunächst in *Stillarbeit*, im Anschluss daran kann eine *Leseübung* zur *Festigung der Aussprache* erfolgen sowie *unbekanntes Vokabular semantisiert* werden. Die **Assignments** festigen das Fachwissen und geben Sprech- und Schreibanlässe.



Aufgabe 1: Die Schülerinnen und Schüler sollen zunächst im *Unterrichtsgespräch* über ihre eigenen Kenntnisse und Erfahrungen mit Malware berichten.



Aufgabe 2: Sodann sollen – **alternativ** nach einer vorangehenden *Gruppenarbeitsphase* – einige Anzeichen und Symptome von Malware beschrieben werden.
Aufgabe 3: Schließlich erarbeitet sich die Klasse erneut im *Plenum* eine kurze Definition von Malware.
Aufgabe 4: Den Abschluss soll ein *Schülervortrag* über die Gefahren von Malware und den Schutz vor ihr bilden.

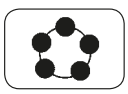


Aufgabe 5: Ein *cartoon* regt die Schülerinnen und Schüler zur *schriftlichen Auseinandersetzung* mit dem Thema und zur eigenen *Meinungsäußerung* an.

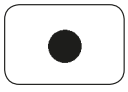
3. Schritt: Personal Data Protection in the Internet

Im Text *"Save for later"* von **Texte und Materialien M 4$_{(1–3)}$** wird das Verhalten von Jugendlichen in sozialen Netzwerken thematisiert. Insbesondere wird in dem Text eine frische Perspektive eingebracht, die genau spezifiziert, was und wie Jugendliche tatsächlich im Internet veröffentlichen und welche Strategien sie dabei verwenden.

Der Text ist inhaltlich und sprachlich komplex. Er enthält zum einen starke kolloquiale Elemente, kombiniert dies jedoch mit statistischen Daten und Fachtermini. Die **Assignments** greifen einzelne Aspekte des Textes auf.



In **Aufgabe 1** wird die Überschrift des Textes *"Save for later"* thematisiert. Die Schüler sollen vor dem ersten Lesen des Textes *diskutieren*, was die Überschrift bedeuten könnte.



Dann lesen die Schüler den Text abschnittsweise in *Stillarbeit*. Den ersten Absatz des Textes sollen sie gemäß **Aufgabe 2** in eine *grafische Veranschaulichung* überführen (z.B. *pie chart* oder *bar chart*). Hierdurch werden gezielt die *Kompetenzen des Lesens* und *Verstehens von statistischen Angaben* gefördert. Die informativen Ausführungen

von **Texte und Materialien M 5** zu Kreis- und Säulendiagrammen können den Schülerinnen und Schülern helfen, diese *Aufgabe selbstständig* zu bewältigen.

In **Aufgabe 3** sollen sich die Schüler mit der *Definition* von *Fachvokabular* auseinandersetzen.
Die **Aufgaben 4 bis 6** beziehen sich auf Zitate im Text, bei denen die Schülerinnen und Schüler aufgerufen sind, jeweils ihre persönlichen *Meinungen zu äußern*.
Aufgabe 7 geht auf Edward Snowden ein, der der Klasse sicher bekannt ist. Diese Aufgabe bietet sich als *Hausaufgabe* an, bei der die Schüler über Edward Snowden *recherchieren* sollen. In der Recherche sollen die Schüler *Argumente zusammentragen,* die für oder gegen das Verhalten von Edward Snowden sprechen. Aus diesen Argumenten (und selbstverständlich auch aus der eigenen Perspektive) sollen die Schüler einen *Kommentar verfassen*, an dessen Ende sie zu einer eigenen Position gelangen. Je nach Leistungsstand der Lerner ist es sinnvoll, mit ihnen vorher noch einmal die *Kompetenz "writing a comment"* zu thematisieren.

4. Schritt: Facebook – Terms and Conditions

Im vierten Schritt (**Texte und Materialien M 6$_{(1+2)}$**) wird die Thematik Facebook aufgegriffen, womit die Schülerinnen und Schüler zumindest oberflächlich vertraut sein sollten. Es geht im Wesentlichen um die allgemeinen Geschäftsbedingungen von Facebook, die den meisten Jugendlichen wohl unbekannt sind. Die Lerner sollen dafür sensibilisert werden, welche Rechte sie den sozialen Netzwerken einräumen bzw. welche Rechte über ihre Daten sie vermeintlich abtreten.

Die sieben **Assignments** dazu gehen detalliert auf die Inhalte von allgemeinen Geschäftsbedingungen ein, verlangen von den Schülerinnen und Schülern die Bewältigung von *Mediationsaufgaben*, beziehen in *Unterrichtsgesprächen* aktuelle Probleme mit ein und schließen ab mit der *handlungsorientierten Aufgabe,* zu beschreiben, wie man einen Facebook-Account löscht.

5. Schritt: Identity Theft in the Internet

In diesem Schritt geht es um eine der größten Bedrohungen des Internets, nämlich den Identitätsdiebstahl. Der Text ist aufgeteilt in zwei Teile. Es wird empfohlen, sie nacheinander lesen zu lassen. **Alternativ** kann die Lehrkraft die Klasse auch in zwei *große Lesegruppen* einteilen und *shared reading* mit ihnen praktizieren. Nach der Lektüre und der Erledigung der dazu gestellten Aufgaben berichtet jede Gruppe der anderen in einem *Schülervortrag* über das Gelesene.

Im **Assignment** zum ersten Teil (**Texte und Materialien M 7$_{(1)}$**) geht es um das Phänomen Identitätsdiebstahl im Internet sowie um *globales Textverständnis*.

Im zweiten Teil (**Texte und Materialien M 7$_{(2+3)}$**) werden die Handlungsschritte der "Online-Diebe" beschrieben. Die **Assignments** setzen auch hier beim *Textverständnis* an. Abschließend (**Aufgabe 4**) wartet auf die Schüler eine *Kreativaufgabe*, in der sie fiktiv eine Polizei-Kampagne gegen Identitätsdiebstahl planen sollen. Die Schülerinnen und Schüler können diese Aufgabe mit eigenen *Postern* oder *Flyern* anreichern.

Is Your Computer Safe?

Assignments:

1. *What can you see in these pictures? Describe them.*
2. *The first picture is a metaphor. What is its message? Give a short answer to this question.*
3. *The second picture is a cartoon. Interpret it.*
4. *Do you know how to make your computer safe? Surf the Internet for answers and discuss this issue with the class.*

(Source: www.variancenet.com/wp-content/uploads/2013/08/computersecurity.jpg)

"Yes, you have done an excellent job of keeping our computer safe.
But sooner or later you`ll have to plug it in."

(Source: www.glasbergen.com/wp-content/gallery/famcom/famcom90.gif)

Eight Ways to Keep Your Computer Safe

With hackers, spammers, and viruses lurking around every corner, you can't afford not to follow some basic steps in protecting your PC and your personal information.

Here are the 8 ways to keep your computer safe:

1. Update your OS
2. Install anti-virus and update
3. Use anti-spyware/adware
4. Secure your home network
5. Use a firewall
6. Don't use IE
7. Watch out for email attachments
8. Keep your personal information safe

1. Update Your Operating System (Windows Update)

The first thing you should do, after getting a new PC or reformatting, is to run Windows Update. […] Whichever operating system you are using, make sure to update them frequently. Especially if you're running Windows, I recommend that you turn on the auto-update in 'Windows Update' if not already done so. Microsoft releases frequent vulnerability and security fixes.

Keeping your operating system up to date is the first step in keeping your computer safe. To check if you're covered (in Windows), open up your control panel and click on Windows Update. If you see the automatic update option selected, you're all set. If not, either choose the full auto update or the option that gives you the chance to choose which updates to install yourself. Just don't turn it off. If you must turn it off for whatever reason, manually check the Windows Update website at least once a week.

Recommended: Try out Ubuntu, the most popular Linux distro. Using a Linux OS may sound too nerdy for some, but the level of user-friendliness has gotten a lot better over the years. It has all the pretty GUI, too. And, if you're having problems, a huge online community is waiting to help you. It's FREE and SAFE.

2. Install Anti-Virus and Keep the Virus Definitions Up-to-Date

An anti-virus software is a MUST. If you don't have one, you are almost guaranteed to get infected; it's only a matter of time. It is amazing how many people don't have an updated anti-virus running on their computers. Especially if you bought a pre-assembled PC from Dell or HP or Acer etc., your computer may come with a free trial period of 30 days to 1 year. Be mindful of this when you purchase a new PC. When your subscription period runs out, you will need to either pay to continue using the anti-virus you currently have or get a different anti-virus software. Shop around.

Recommended: There are tons of options out there. But Avast and AVG are two of the best. Why? Because they're free and very effective. Now, if you want more features and protection, you can move up to a paid anti-virus software. I know Symantec and McAfee are two of the dominant players, but I don't recommend them as they take more resources to run and there are others with better detection rates.

How Malware Works

One of the biggest problems that Internet surfers face today on the World Wide Web is malware. Malware is malicious software that is installed on your PC usually without your knowledge and it can enter your PC as a result of surfing the Internet and in a variety of different ways. Once it sneaks into your PC, malware is capable of spying on your surfing habits, logging your passwords by observing your keystrokes, stealing your identity, reading your email, hijacking your browser to web pages that "phish" for your personal information, and a variety of other invasive tactics.

How To Tell If Malware Has Entered Your PC

Malware is very sneaky about entering your PC. It can enter as the result of clicking on website links, pop-up ads, or any other kind of normal surfing activity. There are subtle and blatant signs that will tell you if it has entered your PC. If you know what to look for, you can easily discover malware and remove it with your antivirus program.

These Are A Few Of The Signs That Malware Has Entered Your PC:

- You start seeing an excessive amount of pop-up ads.
- Your PC's operating system slows down significantly.
- The amount of spam you receive in your email increases.
- Your email account may send out messages to your contact list that you did not send. Sometimes it contains pornographic material or even a trojan or worm.
- The home page you have set in your browser is altered.
- When you try to access a web page in your favorites list, another web page appears that contains advertising or content that encourages you to enter your personal information.
- Your computer completely crashes.
- You are unable to access your antivirus program to remove the malware.

The Origin of Malware and How It Works

Malware is created by criminals that are very sophisticated in computer programming before they install it on the Internet. Malware attaches itself to the components of a web page, pop-up advertisements, toolbars, free stuff that you download, and games, to name a few. When you click on these components, malware sneaks into your computer.

Once malware is in your computer it can steal anything from your music lists to more serious information like your login passwords, bank account numbers, and personal information.

How To Avoid Malware

Although malware is really sneaky, you can help to avoid getting malware by being cautious with your Internet surfing habits and by keeping your antivirus program updated. It is also a good idea to activate the firewall protection. Also, make sure your antivirus program includes malware and spyware protection.

When you surf the Internet avoid clicking on pop-up advertisements regardless of how tempting they may seem. Pay attention to the "Site Advisor" in your antivirus program that will tell you if there are any problems with the website you are visiting.

Make it a general practice to only click on links for websites that you trust, do not volunteer any of your information on unknown websites, and avoid downloading free software from sites you are unfamiliar with.

(Source: http://www.spamlaws.com/how-malware-works.html)

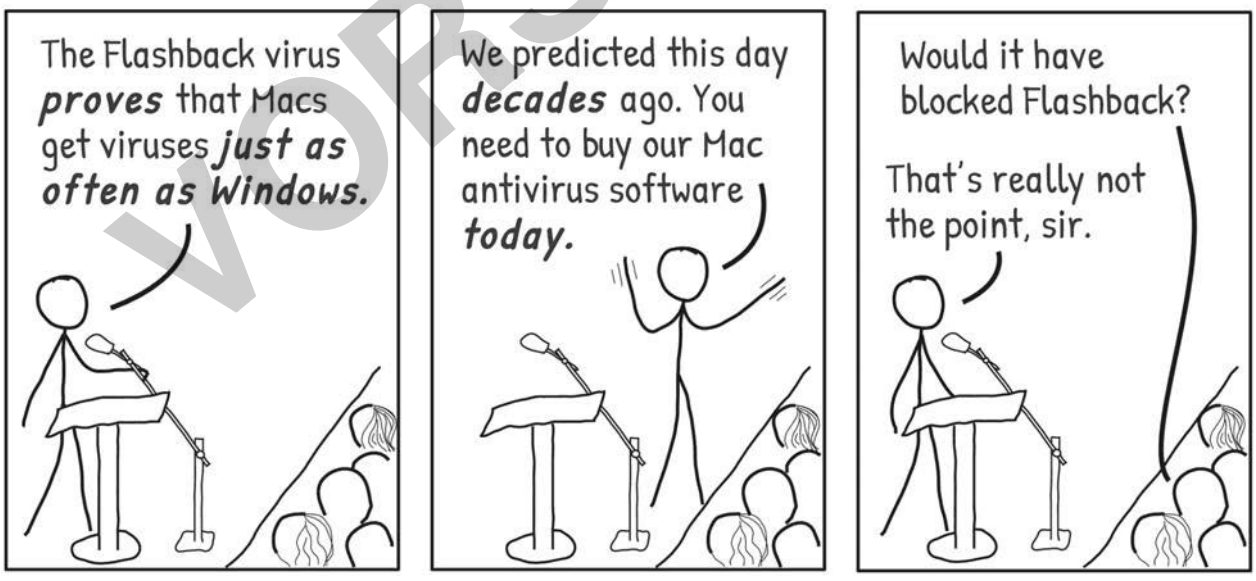
Texte und Materialien – M 3(2)

Annotations:

2 **malicious:** intended to cause damage to a computer system, or to steal private information from a computer system; 4 **to sneak:** to go somewhere secretly, or to take someone or something somewhere secretly; **habit:** something that someone often does; 5 **hijacking:** to take control of or use something that does not belong to you for your own advantage; 9 **sneaky:** used to describe something you do, eat, or drink, especially when you do it without telling anyone or when you should not really do it; 10 **subtle:** small but important; **blatant:** very obvious and intentional, when this is a bad thing; 14 **excessive:** too much; 25 **sophisticated:** *here* intelligent or made in a complicated way and therefore able to do complicated tasks; 26 **to attach:** to fasten, join, or connect something; 32 **cautious:** a cautious action is careful, well considered, and sometimes slow or uncertain; 36/37 **tempting:** if something is tempting, you want to do or have it; 39 **to volunteer:** to offer to do something that you do not have to do, often without having been asked to do it

Assignments:

1. *Do you have any experience with malware? Tell the class about it.*
2. *Describe the signs which might be symptoms of malware that has entered the computer.*
3. ***Team work:** Come up with a short definition of malware which consists of max. two sentences.*
4. *Give a short presentation on the dangers of malware and how to avoid it.*
5. *Have a look at the following cartoon. Write a statement in which you express your opinion on its meaning.*

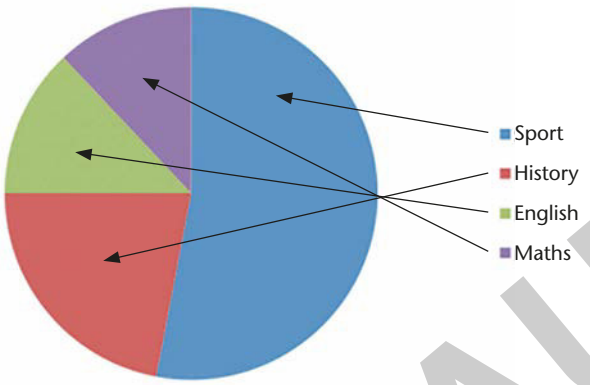


(Source: http://galleryhip.com/having-a-flashback-cartoon.html)

Additional information: Pie Charts and Bar Charts

Pie charts are used in data handling and are circular charts divided up into segments which each represent a value.

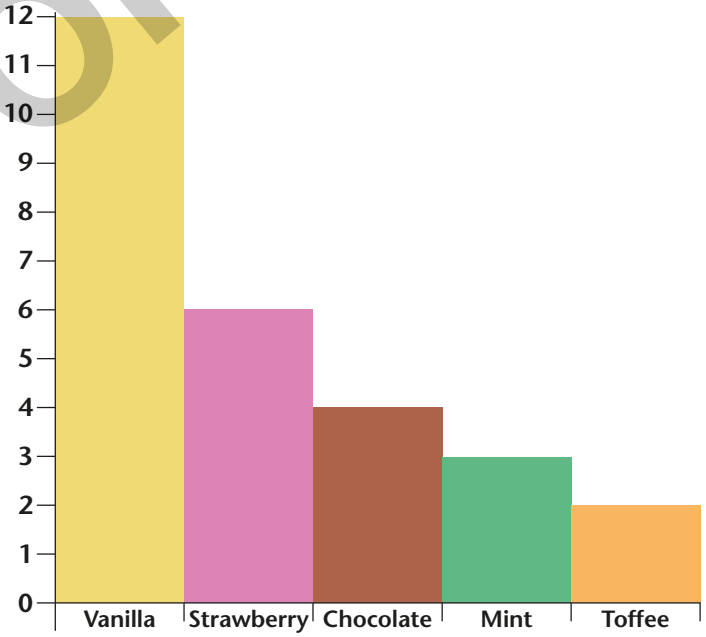
Pie chart



Pie charts are divided into sections (or 'slices') to represent values of different sizes. For example, in this pie chart, the circle represents a whole class. Each member of the class was asked what their favourite subject was, so each segment of the circle represents a different favourite subject: Pie charts are a visual device to help us understand data more easily. For example, in this pie chart we can see that sport was the most popular subject as more than half of the class said it was their favourite subject.

Bar chart

A bar chart displays information (data) by using rectangular bars of different heights.
A bar chart has a vertical axis with numbers on it, and a horizontal axis showing values of something that has been investigated:



(Source: http://www.theschoolrun.com/what-is-a-pie-chart; http://www.theschoolrun.com/reading-bar-chart)

My identity was stolen on Facebook – Part 1

A leafy suburb of South-West London and one morning last November a letter drops on the doormat of Victoria Sennitt's family home. It's addressed to the 24-year-old university graduate and is from a mobile phone company welcoming her to a new contract and explaining the ins and outs of the deal she has just signed up to.

All very friendly – except for the fact that Victoria hasn't a clue what they are talking about. For, as it would subsequently transpire, she has just had her identity stolen: 21st-century style. Forget rummaging through bins, intercepting post or cloning credit cards. All the modern-day crook needs is a computer and an internet connection.

The rest could hardly be easier. Thanks to the ever-growing popularity of so-called social networking sites such as MySpace, Bebo and Facebook, the internet is simply awash with the personal details of millions of potential fraud victims. When Victoria joined Facebook she assumed she was signing up to become part of a fun community where she could meet old friends and make new ones from the comfort of her home.

To aid the process she filled in her online profile with as much detail as possible – adding her e-mail address, home address, phone numbers and even her date of birth.

"The ironic thing is that in the real world I am really careful with sensitive personal information," she says. "I shred anything that might be of use to anyone; all my correspondence, my old bank statements, bills and documents.

"But for some reason when I signed up to Facebook it felt as if I was joining something self-contained, something that would be used by like-minded people. Only now do I realise how wrong I was. "The truth is that you don't know who anyone is on the internet and you don't know what their motives are for using it. I know it sounds stupid, but I feel very violated to know that a criminal was able to log on to my page and steal my personal details."

In a way Victoria was lucky. With a few phone calls she managed to persuade the phone company that a fraudster, assuming her identity, had set up the contract. Had she failed to notice the deception, no doubt her identity would have been exploited over and over again.

Already in the UK, identity fraud is estimated to cost the economy £1.7 billion a year and the evidence is that the criminals are growing more sophisticated every year. Experts warn that their focus has shifted on to the internet with teenagers and young men and women targeted. Not only are they more likely to belong to these social networking sites, but they are by nature more free and easy with their personal information and less likely to keep close track of their financial affairs. But it is not just these sites that are being mined for information. Planning applications posted by local authorities, CVs entered on recruitment websites, websites reuniting old school-friends – they are all meat and drink to the cyber criminals.

Assignment:

Read the text for global understanding. Then do the tasks and answer the questions.

a) *What has happened to Victoria? Retell the beginning of the story.*
b) *Explain the process of how identity theft works.*
c) *Describe the role that Facebook plays in this crime.*
d) *Explain what the following phrase means: "But for some reason when I signed up to Facebook it felt as if I was joining something self-contained, something that would be used by like-minded people." (lines 19–20)*
e) *Explain what this phrase means: "[…] they are all meat and drink to the cyber criminals." (line 34)*