

Online Safety



> **Getting Started: Vocabulary** (page 134)

1 Read the online advice page. Then decide which tips on the right are mentioned in the article. ◀

Tips:

1. Don't give your passwords to other people.
2. Use a different password for each account.
3. Use privacy control. Only let certain people view your personal details.
4. Report spam to your e-mail client.
5. Use filters to reduce spam.
6. Check your children's use of the Internet and social media.

How to Stay Safe Online

BLOGS **ADVICE** CONTACT

With more and more people completing transactions online, digital safety has become an important factor. Today, more than ever, you must take precautions to ensure your personal information is safe from hackers and thieves.

1 PASSWORD PROTECTION:

- Never share your passwords with anyone or include them in e-mails.
- Password protect all sensitive files on your computer.
- Use a sentence that is at least 12 characters long to create a strong password.

2 SOCIAL MEDIA:

- Protect against identity theft. Don't make your personal information public.
- Adjust your privacy settings to limit who can see your profile. If you don't want to risk everyone seeing your photos, don't post them online at all.
- Don't make your holiday plans and live photos public. Thieves will know when your house is empty.

3 E-MAIL:

- DON'T open, click on a link or reply to an e-mail if you don't know who sent it to you.
- Use filters to block unwanted e-mails such as:
 - i. Phishing – fake or fraudulent e-mails to trick users into sharing their personal information like credit card details, user names and passwords.
 - ii. Bulk e-mails – e-mails sent to millions of people. They may contain links or downloads with viruses or spyware which can corrupt your computer.

4 SAFETY FOR CHILDREN:

- Use parental control options to block undesirable websites, videos and content.
- Monitor your children's use of social media and browsing.
- Instruct young children and teens about online safety. Teach them not to 'make friends' with everyone. People may hide behind a false identity.

2 Two colleagues are discussing Internet security. Choose the correct answer. Then listen to the dialogue and check your answers. ◀

- A:** Hi, Katie. My daughter was surfing the web last night and I noticed some undesirable content that I didn't want her to see. I need to block certain ¹ e-mails / websites. Do you know how I can do this?
- B:** It's easy, Wendy. You can set up your PC to monitor what your children are viewing. It will also keep them away from certain games and sites. You can even set limits on how much time they spend online.
- A:** You mean I can actually ² limit / decide what sites the browser finds?
- B:** Sure. Almost all browsers and social media websites have Parental Controls or Privacy Settings.
- A:** Where do I find the Parental Controls on Google? How do I ³ set / do them?
- B:** In your browser, go to Search Settings on the right-hand side of the screen. Under "SafeSearch filters", check the box next to "Turn on SafeSearch". Then at the bottom of the page, click "Save".
- A:** How does this help?
- B:** When someone does a search in their browser, this filters the search results and eliminates undesirable videos and websites.
- A:** Is it completely ⁴ safe / sure?
- B:** It's not 100% accurate. However, it helps protect children from most of the ⁵ relevant / inappropriate search results.

3 Practise the dialogue in Exercise 2 with a partner. Pay attention to the sentences in colour.

4 Read the dialogue in Exercise 2 again. Then match A to B to form sentences.

A

1. Wendy
2. Katie
3. A SafeSearch filter
4. Many social media sites



B

- a. may not eliminate all inappropriate material.
- b. didn't know that parents can limit online access.
- c. have got parental controls.
- d. recommends filtering search results.

Working with Vocabulary

5 Match A to B to make expressions. Then listen and repeat the expressions. (4)

A

1. identity
2. parental
3. make
4. privacy
5. password

B

- a. settings
- b. public
- c. protect
- d. theft
- e. control

6 Copy and complete the sentences below with the expressions from Exercise 5.

1. Think twice before you your private information
2. Using, you can adjust what different people see on your Facebook page.
3. is a very serious crime.
4. your account with a combination of letters, numbers and symbols.
5. Fathers and mothers should think about putting onto the family PC.

7 Listen and repeat the words in colour. Then choose the correct answer. (4)

1. A **hacker** / **profile** contains a person's personal information.
2. Using another person's credit card without permission is **fraudulent** / **undesirable**.
3. It's important to **ensure** / **hide** your children are safe on social networking sites.
4. A firewall can **trick** / **block** unauthorised users from accessing a network.
5. Do you think parents should **post** / **monitor** their children's access to the Internet?
6. Viruses can **corrupt** / **risk** the information on your computer files.

8 Listen and repeat the words in colour. Which pairs of sentences have got a similar meaning? (4)

1. a. You should delete an e-mail that seems suspicious.
b. If you don't know the source of an e-mail, throw it out.
2. a. **Phishing** messages look like they come from a reputable company.
b. Reputable companies send messages as a way of getting more customers.
3. a. **Adware** collects information about users' Internet activities.
b. Adware analyses which websites a user visits.
4. a. **Thieves** can use your credit card details to purchase products from websites.
b. Most people use their credit cards to purchase online today.
5. a. Companies often send out **bulk e-mails**.
b. To get to all their clients, companies send out thousands of e-mails at the same time.

9 Match A to B to form sentences.

A

1. You could meet undesirable people
2. A hacker can change
3. Fake e-mails can trick users into
4. Learn how to hide your online identity
5. You can post a helpful reply
6. You risk losing your privacy

B

- a. giving away vital information.
- b. on social networking sites.
- c. when you share too much personal information.
- d. on this forum.
- e. and be anonymous on the web.
- f. information on your computer system.


Your Turn


Listen to the conversation between a bank employee and a client. Copy and complete the chart. Then tick (✓) the correct columns. (4)

Who ... ?	Client	Bank Employee
1. reported the scam		
2. was suspicious because of the logo		
3. knew about the phishing		
4. wanted to prevent this from happening again		
5. will adjust the filters		

Protecting Your Business

> *Getting Started: Vocabulary (page 134)*

- 1 Read the e-mail. Then choose the correct answers to the questions on the right according to the text. 

 To: IT Managers
From: Sam Brown: Network Administrator
Subject: Company Cyber Security Meeting

Following last week's cyber attack attempts, we all need to reassess security to protect our business. Please read the agenda points below before our meeting. It is essential that ALL managers attend.

1. Establish better network security: Buy new antivirus software with 'real-time' protection to make sure we are better protected against viruses, spyware and other malicious codes. Check which new vendors regularly provide patches and updates to their software.

2. Secure our network: Check the firewall and encrypting information. Make sure the WiFi is secure and hidden. To safeguard from unauthorised access, implement password protection on the router.

3. Establish stronger security policy for all employees: Consider implementing multi-factor authentication for employees to gain entry to sensitive data. Administrative privileges should be limited to IT managers only. Make sure all employees are aware of the penalties if they violate the business' cyber security rules.


4. Research new backup system: Install a more innovative program to perform daily backup which also includes an effective recovery solution. An alternative backup for storing copies off-site or on the cloud is also essential.

5. Redesign policy on payments: Check our authentication system with the bank and credit card companies before we open our e-commerce site. It is imperative we use the most trusted validation tools and anti-fraud services.


Tip!

Multi-factor authentication combines two or more independent credentials: something the user knows, such as a password or a secret question; something the user has got, such as a bank card; and biometric verification.

- Sam Brown is insisting that
 - IT managers participate in the meeting
 - all employees read the agenda
- Sam Brown believes that the company needs to
 - update its antivirus software
 - replace its antivirus software
- The company has got cyber security rules
 - which allow employees to see all data
 - which employees mustn't violate
- The company would like a backup program which
 - provides a way to recover data
 - stores data on the cloud
- The company is planning to
 - sell products online
 - redesign their products

- 2 An IT security advisor (A) is giving security advice to a business owner (B). Number sections A-C in the correct order to form a dialogue. Then listen to the dialogue and check your answers. 

- A B: Yes. How else can we make sure our network is completely secure?
A: You should consider installing a VPN – a virtual private network. It offers a much better level of security.
B: How does that work?
A: It works as a private network, even though you are using a public network.
-
- B A: Hi, Mathew. What seems to be the problem?
B: Well Jack, last month we had a serious security breach even though we had installed new anti-virus software.
A: When did you last download an update?
B: Oh! I'm not sure.
A: You need to check for software updates at least once a month.
-
- C B: OK, I'll get the IT staff to check that.
A: Is there anything else that you're concerned about?
B: Yes, some employees have complained that sometimes they can't access all the programs they need.
A: It sounds like we need to reassess the firewall settings. I'll adjust the settings for you. Have you got any other questions?

-  3 Practise the dialogue in Exercise 2 with a partner. Pay attention to the sentences in colour.

4 Read the dialogue in Exercise 2 again. Then decide whether the sentences are true, false or the text doesn't say.

1. Mathew's company has got new anti-virus software.
2. Mathew updated his new anti-virus software last month.
3. Employees now get increased access to more programs.
4. Adjusting the firewall settings will prevent the employees from accessing programs.
5. Jack recommends reducing risk by using a private network.

Working with Vocabulary

5 Listen and repeat the words in colour. Then replace the words in bold with the words in colour. ◀▶

safeguarded • gain entry to • establish agenda • attempted

1. We weren't able to **get into** the factory.
2. The manager wanted to **create** a new department.
3. Hackers **tried** to get into the bank's network.
4. Before the meeting, we received the **list of the topics to discuss**.
5. Make sure your computer is **protected** from malware.

6 Listen and repeat the words in colour. Then match A to B to form sentences. ◀▶

A

1. A cyber attack on a government
2. E-commerce is a business transaction
3. If we **encrypt** all the customer data,
4. **Malicious code** is used to
5. Special data recovery software
6. **Tools** are a set of basic accessories
7. A **VPN (Virtual Private Network)** is a private network

B

- a. for software developers.
- b. can help you find deleted files.
- c. damage data, files and computing systems.
- d. over the Internet.
- e. built over a public infrastructure.
- f. it will be protected.
- g. can cause chaos.



7 Listen and repeat the words in colour. Then use them to complete the dialogues. ◀▶

1. real-time protection • aware of multi-factor authentication

A: Is your network secure?

B: Yes. I am ¹..... the problem, so I've got some good ².....

A: Have you considered using ³.....?

B: Yes, I have, but I've decided not to do that at the moment.

2. penalty • reassess • breach • sensitive

A: We had a data ⁴..... last week, so our company is very ⁵..... about security. I can't give you my password.

B: What's the ⁶..... for doing this?

A: The manager will ⁷..... my contract and I could find myself without a job.

8 Choose the correct answer.

1. This is *sensitive* / *trusted* information, so please don't discuss it with anyone.
2. Releasing this information is considered a security *tool* / *breach*.
3. You need to *safeguard* / *attempt* your network against unauthorised entry.
4. What is the *penalty* / *agenda* for coming late to work?
5. Hackers were able to *gain entry to* / *establish* the accounting system.

Your Turn

Student A: You are a security administrator. Ask your security advisor to help you solve some problems. Use the chart on page 91 to tell him / her your problems and record the solutions.

Student B: You are an IT security advisor. Provide solutions for your client using the information on page 99.



18 Vocabulary and Functional Language

1 Circle TWO correct answers.

Which of the following ... ?

1. are criminals
 - a. hacker
 - b. adware
 - c. thief
2. can cause harm
 - a. profiles
 - b. phishing messages
 - c. identity theft
3. provide security
 - a. bulk e-mails
 - b. parental control
 - c. privacy settings
4. should be done to stay safe online
 - a. block spam
 - b. make your personal details public
 - c. password protect

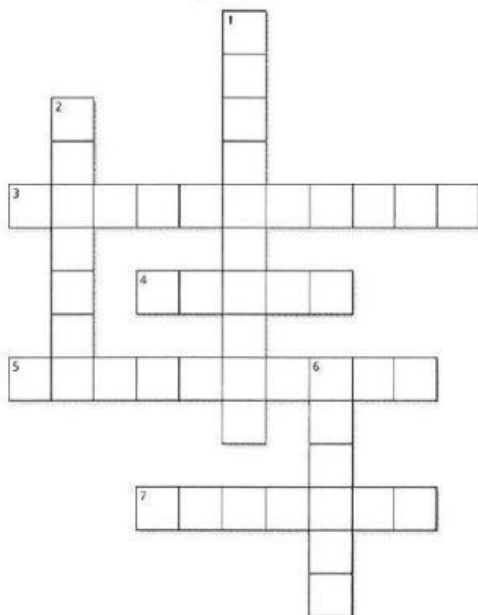
2 Complete the puzzle according to the clues.

Across →

3. Many parents block their children from ... activities online.
4. A scam is when someone tries to ... you.
5. Unauthorised access to a company's files is ...
7. You cannot usually open a file that is ...

Down ↓

1. If an e-mail looks ... , don't open it.
2. Do you think parents should ... their children's Internet activities?
6. Most companies ... their files are backed up at the end of the day.



3 The words in bold are in the wrong sentences. Write them next to the correct sentences.

1. Some companies send **profiles** to tell their customers about an event.
2. **Adware** can happen if you don't keep your personal information private.
3. You don't **post** losing money if you buy from a reputable company.
4. Registered users create **bulk e-mails** on social networking websites.
5. Gamers often **risk** their real identity when playing games online.
6. **Identity theft** is offered to customers who don't want to pay for software.
7. People sometimes **hide** a question on a forum when they need advice.

4 Complete the correct word or phrase next to its definition.

1. the act of getting back something lost
r.....
2. to start something such as a company
e.....
3. something that causes data theft
m..... c.....
4. to examine or think about something again
r.....
5. a violation
b.....
6. doing business over the Internet
e.....
7. reveal, make known
m..... p.....



5 Circle the correct continuation. Pay attention to the words in bold.

1. An **agenda** tells us ...
 - a. the time and place of the meeting
 - b. what we will discuss at the meeting
2. There is a **penalty** if you ...
 - a. reschedule your visit
 - b. don't pay on time
3. The passwords are **encrypted** in order to ...
 - a. enrich the program
 - b. provide full security
4. **Real-time protection** should ...
 - a. protect your computer from all viruses
 - b. update your database
5. **Cyber attacks** use damaging codes and malware to ...
 - a. install important information
 - b. change computer data
6. In order to **gain entry to** the system, you must ...
 - a. have the correct password
 - b. have a third-party program

6 Complete the sentences with the words and phrases below.

- virtual private network • safeguarded
 attempted • tools • sensitive
 multi-factor authentication • aware of
1. To get money out of my bank, I need – my bank card and a password.
 2. We weren't the problem until we tried to get into the Internet.
 3. Hackers to steal data from our customers.
 4. These are documents, so please don't make them public.
 5. If the system isn't, it may be accessed by unauthorised users.
 6. Companies use a to communicate confidentially over a public network.
 7. I used these drawing to create the poster.



Say It!

Write the sentences in your language.

1. Is there anything else that you're concerned about?

2. It's not 100% accurate.

3. When did you last download an update?

4. It sounds like we need to reassess the firewall settings.

5. You need to check for software updates at least once a month.

6. You can set up your PC to monitor what the children are viewing.

7. A VPN network offers a much better level of security.

8. I'll adjust the settings for you.

ONLINE SAFETY

adware	parental control
block	password protect
bulk e-mails	phishing
corrupt	post
ensure	privacy settings
fraudulent	profile
hacker	risk (v)
hide	suspicious
identity theft	thief (thieves)
make public	trick
monitor	undesirable

> **before page 74**

CYBER SECURITY

agenda	multi-factor authentication
attempt	penalty
aware of	real-time protection
breach	reassess
cyber attack	recovery
e-commerce	safeguard
encrypt	sensitive
establish	tools
gain entry to	VPN (Virtual Private Network)
malicious code	