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

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.

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.

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 **Then listen and repeat the expressions.**

A	B
1. identity	a. settings
2. parental	b. public
3. make	c. protect
4. privacy	d. theft
5. password	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.**

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?**

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.

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		

> *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;

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

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.