5. Safely Using Email and Purchasing Items on the Internet

Are you receiving a lot of unwanted email every day? For example, phishing messages, spam, hoaxes, or chain letters. Nowadays, many of these types of messages will be blocked by your email service provider, but you can take steps yourself to prevent and delete unwanted email. In this chapter we provide some useful tips on how to do this.

You can order and pay for products and services online in a webshop. As you surf the Internet, it may seem amazing how easy it is to buy things right from your armchair, and in most cases, have them delivered to your front door.

There are various ways to pay for products and services you buy online. The seller determines the payment methods on offer. As a buyer, you need to agree to these methods. It is important to pay attention to the security issues regarding online payments, and you need to take the time to read the terms of delivery and warranty.

In this chapter you will learn more about the issues involved in making online purchases, such as recognizing a secure website and the payment methods being used. You can just read this information as a means to help you make informed decisions. Then you will know what to take into account when you purchase something yourself.

In this chapter you will get information on:

- phishing, spam, hoaxes, and chain letters;
- safe mail behavior;
- safe online shopping;
- payment methods on the Internet;
- identifying a secure website.

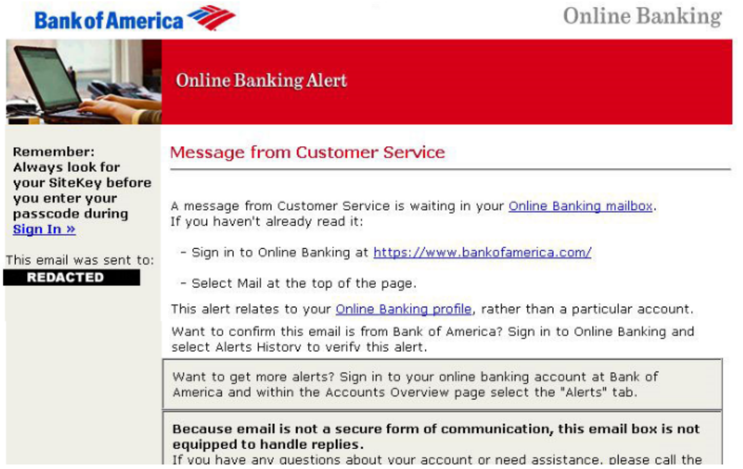
5.1 Phishing

Phishing is a method of persuading unsuspecting computer users to disclose their personal data or financial information by posing as a legitimate person or organization. In fact, phishing is a way of ‘fishing’ for information.

A familiar tactic in phishing is to send a fake email message that looks like a real message sent by a familiar, trusted source. This might be your bank, Credit Card Company, a web store, or another website you have previously visited. These fake messages are sent to thousands of email addresses.
In the email, the recipients are asked to check their bank data, for instance. The message contains a hyperlink for this purpose. If the link is clicked it may lead you to a website that may look like a bank’s website. There you will be asked to enter personal information, such as name and address, bank account numbers, and PIN codes, supposedly to check if everything is OK.

An example of a phishing mail:

This email asks the clients from this bank to enter their personal information on a certain website. Criminals can then gain access to these accounts and empty them out.



Bank of America Online Banking

Online Banking Alert

Remember: Always look for your SiteKey before you enter your passcode during Sign In »

This email was sent to: REDACTED

Message from Customer Service

A message from Customer Service is waiting in your Online Banking mailbox.
If you haven't already read it:

- Sign in to Online Banking at https://www.bankofamerica.com/
- Select Mail at the top of the page.

This alert relates to your Online Banking profile, rather than a particular account.

Want to confirm this email is from Bank of America? Sign in to Online Banking and select Alerts History to verify this alert.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

Because email is not a secure form of communication, this email box is not equipped to handle replies.
If you have any questions about your account or need assistance, please call the

If you fall for this trick and enter your data, the information will be sent immediately to the criminals who have set the trap. Next, they may use your data to purchase items, open new credit card accounts in your name, or abuse your identity in other ways. These phishing mails and websites have a deceptively genuine look. They often use the bank’s logo in the email, and the website may look like the legitimate website.

Please note:

Nowadays, Internet criminals have thought of something new: contacting people by phone. One of the phony stories they use, is telling you there is something wrong with your computer. They tell you that the ‘problem’ can be solved if you enter various types of information (often personal data). This is also considered a kind of phishing.

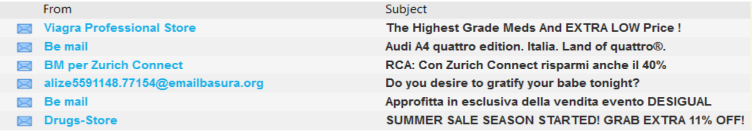
5.2 Spam

By ‘spam’ we mean all those email messages containing unwanted and undesirable ads that seem to land in your inbox on a daily basis. These might be ads for ordering certain medication, online gambling, or shady dating websites.

Spam is intended to lure you to a certain website and get you to buy their products. The websites are usually run by swindlers who deliver worthless or illegal products, or simply do not deliver anything at all, once payment has been received.

Sometimes these messages may have originated from legal foreign companies, but since sending spam is prohibited in more and more countries, the odds of the companies concerned being trustworthy are very small. It is best never to react to this type of advertising email.

Here you see a few examples of spam:



From	Subject
Viagra Professional Store	The Highest Grade Meds And EXTRA LOW Price !
Be mail	Audi A4 quattro edition. Italia. Land of quattro®.
BM per Zurich Connect	RCA: Con Zurich Connect risparmi anche il 40%
alize5591148.77154@emailbasura.org	Do you desire to gratify your babe tonight?
Be mail	Approfitta in esclusiva della vendita evento DESIGUAL
Drugs-Store	SUMMER SALE SEASON STARTED! GRAB EXTRA 11% OFF!

Because there is always a small minority of computer users who react to spam, it is still worthwhile for the spammers to keep sending their spam mail. Sending an email does not cost them a lot of time or money. They often use a network of hacked computers. The computers themselves may have been taken over in an illegal manner and then are used remotely by criminals. This is often how email addresses are obtained.

The annoying thing about spam is that your mailbox can quickly be filled with useless email and it takes a lot of time to get rid of it. Without taking precautions, the amount of unwanted email can increase up to hundreds a day.
Nowadays, Internet service providers use spam filters that block a lot of spam from ever entering your inbox. Because of this you will already receive less spam on your computer. But it is still wise to take your own measures against spam on your own computer. There are antivirus programs that will protect you from spam. The *Mail* email program also has a spam filter option.

Please note:

Not all advertising email is spam. If you have previously signed up with a company and entered your email address, you will most likely begin to receive email from them. If this is a respectable company, there will be an opt out link in the email message (often at the bottom) that will lead you to a web page where you can sign off from this service.

- Continue on the next page -

Keep in mind though, that even some spammers will offer to put a stop to their ads in their emails. They will ask you to click a hyperlink in the email in order to sign out and stop the ads. But instead of signing out, you have in fact sent a confirmation of your email address, which will lead to even more spam. Signing out in this way is only safe if you trust the company because you have previously purchased something with them, or have explicitly given them permission to use your email address.

5.3 Hoaxes and Chain Letters

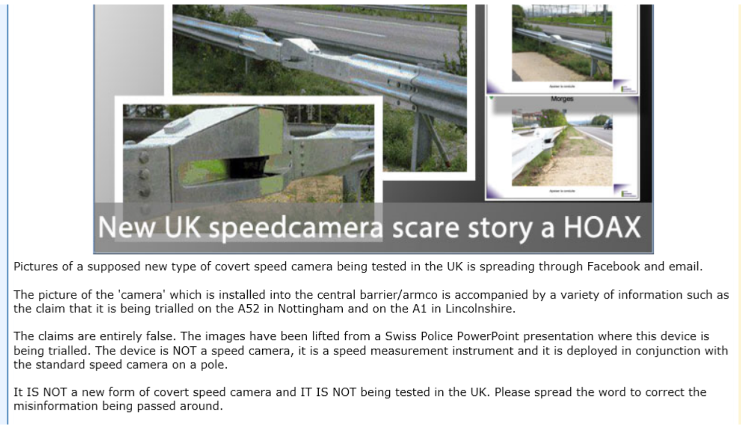
A hoax is a deliberately fabricated falsehood made to masquerade as truth. The Internet is full of these hoaxes. When one is used in an email, it is often in the form of a chain letter.

For example, you receive an email message that tells you to forward this message to ten others as soon as possible. If you do not do this, something bad will happen to you or to your loved ones. This is the digital version of the classic chain letter. Other versions contain a sad story, for instance, about someone who is seriously ill, and can only pay for special treatment if the email is forwarded lots of times. Supposedly some kind philanthropist or corporation will then pay one cent for each email that is forwarded. This type of story is rubbish. The sick person does not exist and the photos in the message have probably been plucked from the Internet. If a company decides to help someone, they will never do it like this.

Sometimes these emails contain an ‘urgent message’ warning you about a dangerous virus on the Internet. They often try to induce you into removing a certain program from your computer. This is usually a program that is essential for the normal working of your computer. If you remove it, you will very likely experience problems with your computer.

If you receive this type of chain letter or hoax, do not forward it. The hoax is primarily intended to gather as many email addresses as possible to be sold or used in future spamming. Many hoaxes and chain letters are also distributed through *Facebook*.

A very well-known hoax is the message warning you against a new type of (fake) speed camera, used by the police. The recipients of this message are asked to ‘behave socially’ and share this message with as many others as possible. Many people will actually believe this.



New UK speedcamera scare story a HOAX

Pictures of a supposed new type of covert speed camera being tested in the UK is spreading through Facebook and email.

The picture of the 'camera' which is installed into the central barrier/armco is accompanied by a variety of information such as the claim that it is being trialled on the A52 in Nottingham and on the A1 in Lincolnshire.

The claims are entirely false. The images have been lifted from a Swiss Police PowerPoint presentation where this device is being trialled. The device is NOT a speed camera, it is a speed measurement instrument and it is deployed in conjunction with the standard speed camera on a pole.

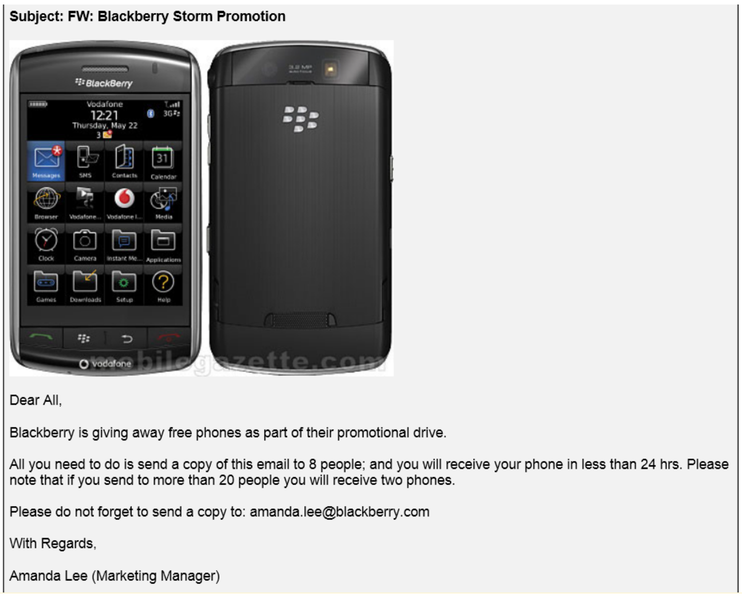
It IS NOT a new form of covert speed camera and IT IS NOT being tested in the UK. Please spread the word to correct the misinformation being passed around.

If you would take the time to search text used in this message on *Google*, you would quickly discover that it is a hoax.

In this example of a phony message you have supposedly won a prize:

You can win this popular gadget by sharing a message and 'liking' a certain web page.

But if you carefully look at the web hyperlink or email address, you will see that this information is not the page or email address from a well-known, legitimate company.



Subject: FW: Blackberry Storm Promotion

Dear All,

Blackberry is giving away free phones as part of their promotional drive.

All you need to do is send a copy of this email to 8 people; and you will receive your phone in less than 24 hrs. Please note that if you send to more than 20 people you will receive two phones.

Please do not forget to send a copy to: amanda.lee@blackberry.com

With Regards,

Amanda Lee (Marketing Manager)

This type of win-a-prize message is usually a scam. The purpose of the scam is to gather as many 'likes' as possible, then empty the page and sell it to others.

If you know what to look for, you can easily spot a fake 'you have won' message:

- the message is often in English with spelling mistakes;
- the message is not linked to the official website or the official *Facebook* page of the manufacturer;
- the *Facebook* page containing the fake message just contains a single message;
- if the offer appears to be too good to be true, it often is!

Another famous hoax features a picture of a wounded or sick child that is used to induce people to share the message with the claim that '*Facebook* will donate one dollar to a good cause for each shared message'… If *Facebook* intends to donate money they will not do it like this! Do not share these kinds of *Facebook* messages!