BE SAFE ON THE INTERNET

Content Unit

[Information Stream and Online Communication]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit schulungscenter
Last processing date: 14.08.2020

Funded by the
Erasmus+ Programme
of the European Union

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Co-funded by the Erasmus+ Programme of the European Union

Information Stream and Online Communication

First Introduction

The Internet massively influenced the way we communicate with each other. For most of us, online communication is simply part of everyday life. Countless e-mails are opened, forwarded and answered. In this way, information can be passed on quickly, easily and cost-effectively. Your e-mail program somehow does not work properly? Let's start browsing the Internet - it's easy to find a forum where someone describes similar problems or other users share useful tips with the online community. As you can see, there is no doubt that online communication offers many advantages. However, the everyday use of e-mails and other electronic means of communication, which is taken for granted, tempts people to become careless and thus to recognise potential risks too late or not at all. This makes it all the more important to know what you should really pay attention to when using online communication to reduce the risk of negative consequences.

Practical relevance – This is what you will need the knowledge and skills for

The increasing use of the Internet and various electronic communication tools - both in our private and professional lives - is creating additional threats to the security of our data and our privacy. It is therefore important to know the current data protection risks in order to be able to recognize them quickly and react correctly if necessary. In times of increasing cybercrime, the appropriate know-how about possible security problems in the course of online communication as well as the correct and secure handling of e-mails is a must for every Internet user.

Overview of learning objectives and competences

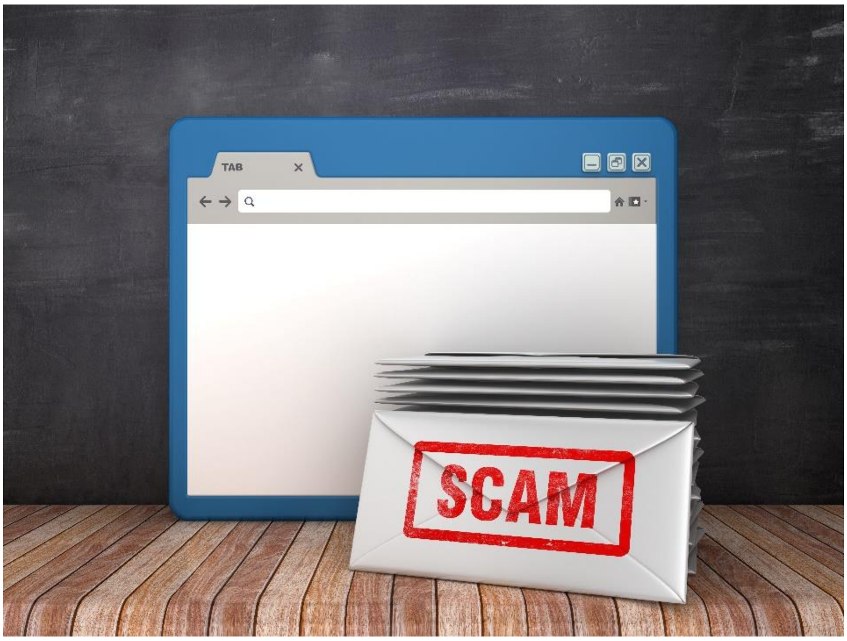
In LO_Information stream and online communication_01 you will learn about the risks of online communication via e-mail and what you should be aware of to avoid these risks. In LO_Information stream and online communication_02 you will learn about the risks of online communication via foren and chat rooms and what you should pay attention to. In LO_Information stream and online communication_03 you will receive some basic information about what you need to pay attention to when communicating on social networks.

Learning objectives	Fine objectives
LO_Information stream and online communication_01: You know about the risks of	FO_Information stream and online communication_01_01: You can explain the term fake e-mails.

online communication via e-mail and what you should pay attention to.	FO_Information stream and online communication_01_02: You can give examples of typical characteristics of harmful e-mails. FO_Information stream and online communication_01_03: You can name some measures that can help to reduce the risk of online communication via e-mail.
LO_Information stream and online communication_02: You know about the risks of online communication via foren and chat rooms and what you should pay attention to.	FO_Information stream and online communication_02_01: You can explain what forums and chat rooms are and how they differ from each other. FO_Information stream and online communication_02_02: You can name potential risks related to communication via forums and chat rooms. FO_Information stream and online communication_02_03: You can name some measures that can help to reduce the risk of online communication via forums and chat rooms.
LO_Information stream and online communication_03: You know at a glance what you need to pay attention to when communicating on social networks.	FO_Information stream and online communication_03_01: You can name some aspects that should be considered in communication via social media to avoid potential negative consequences. FO_Information stream and online communication_03_02: You can explain how to react in case of observed misconduct or abuse of social media.

1.Build knowledge - Fake e-mails and attachments

The **most popular online communication medium is e-mail.** Opening and sending e-mails is most likely also part of your daily routine, isn't it? But precisely because of the high popularity of email communication, **fake emails** are a common threat too.



Definition

Fake e-mails are undesirable e-mails that mislead you in bad faith with deceptive information or lead you to perform harmful acts. For example, malicious programs are often transferred to fake e-mails via **attachments.**

It is therefore important to be aware of the typical characteristics of malicious e-mails. Before opening attachments, clicking on links or answering e-mails, it can be helpful to **ask yourself the following questions**:

1. Are you promised something you think would be **too good to be true**? Be careful: If it's too good to be true, it's most certainly not real.

Example

Examples of this are usually very attractive ladies who want to get to know you, free gifts or the notification that you have won a prize (although you did not take part in any sweepstakes contest).

2. Does the content of the email somehow **not fit with the (supposed) trusted email sender**?

Example

You got an e-mail from your friend Anna. She writes that she is on vacation abroad and has been the victim of a theft. Anna therefore urges you to transfer money immediately to an account so that she can take the last plane back home this week.

Such content clearly indicates that your friend Anna's email account has been hacked.

3. Does the e-mail contain certain **irritating words as the subject-matter**, such as "last reminder", "account blocked" or similar? Are you asked to disclose your access data, passwords or other **confidential information**?

Important

Whenever someone urges you to hurry or disclose confidential information, it should set the alarm bells ringing!

4. Does the **sender seem strange** to you (e.g. you receive an English mail from a German company)? Or does the e-mail contain a lot of **spelling or grammar mistakes** (probably due to automatic translation programs)?

5. Was the email automatically moved to the **spam folder**?

You might be wondering now, why you should even think about spam emails. Many email providers are constantly improving their automated monitoring and therefore unwanted emails automatically end up in the so-called spam folder. The problem, however, is that it can also happen that an e-mail is mistakenly considered to be potentially unwanted and ends up in the spam folder.

Example
Your friend is having a big party for his birthday. He sends the invitations by e-mail to many invitees simultaneously by entering all e-mail addresses under BCC. Unfortunately it is possible that your invitation will end up in spam, since many addresses in BCC are a typical sign of spam mail.

6. Are you prompted to run programs with strange filenames (e.g., compositions of known filenames such as "jpg.vbs" or "gif.exe")?

If you had to answer "Yes" to one or more of these questions, or if a mail seems suspicious to you for other reasons, **you should not open the mail** or the files and links it contains.

So-called **pishing mails** require special caution.

Definition
The term **phishing** consists of the two words "password" and "fishing". Phishing is the attempt to obtain **foreign passwords** with the help of fake e-mails.

You may have already received a **strange e-mail** from your bank or an online shop you know. In many cases you will be informed that your user data has unfortunately been lost or your password has expired or that a new identification is urgently required due to an update. Conveniently, **a link to the company's websit**e is usually sent directly. These web pages look **very similar** to the originals, but they are **fake**. If you enter your bank access data in good faith, the fraudsters will gain access to it and can harm you.

Tip
Mails in which you are requested to disclose your user data should never be answered. Serious companies would not require this. If you are still unsure, it makes sense to ask the alleged sender of the mail by telephone!

Furthermore, the following measures can help to **reduce the risk** of online communication due to emails:

- Activate the **file extension display** (e.g. .docx, .exe). This allows you to identify malicious programs sent as e-mail attachments better.
- Use appropriate security settings to prevent the execution of active content in e-mail programs. For example, you can prevent **unwanted malware** from being run when a mail is opened.
- **Save suspicious attachments first** so that you can scan them with a virus program.

1.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_01

Situation: What is meant by the term "fake e-mail"?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Fake e-mails are unwanted e-mails, which often contain malware sent via attachment.**
- **Fake e-mails often provide false or untrue information.**
- **Fake e-mails may not even have been sent by the alleged sender.**
- Fake emails are emails without any content. These blank emails were sent either intentionally or as an accidental message.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_02

Situation: You check your email account and notice many new emails. Which one of the following cases has a high probability of a fake email?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **You are promised a big payoff.**
- **You are urgently requested to change your access data.**
- The email has no subject.
- **In the subject line is a final warning.**
- **The email contains a noticeable number of spelling mistakes.**
- **The email was automatically moved to the spam folder.**
- The email was sent in the early morning hours.

Exercise MULTIPLE CHOICE

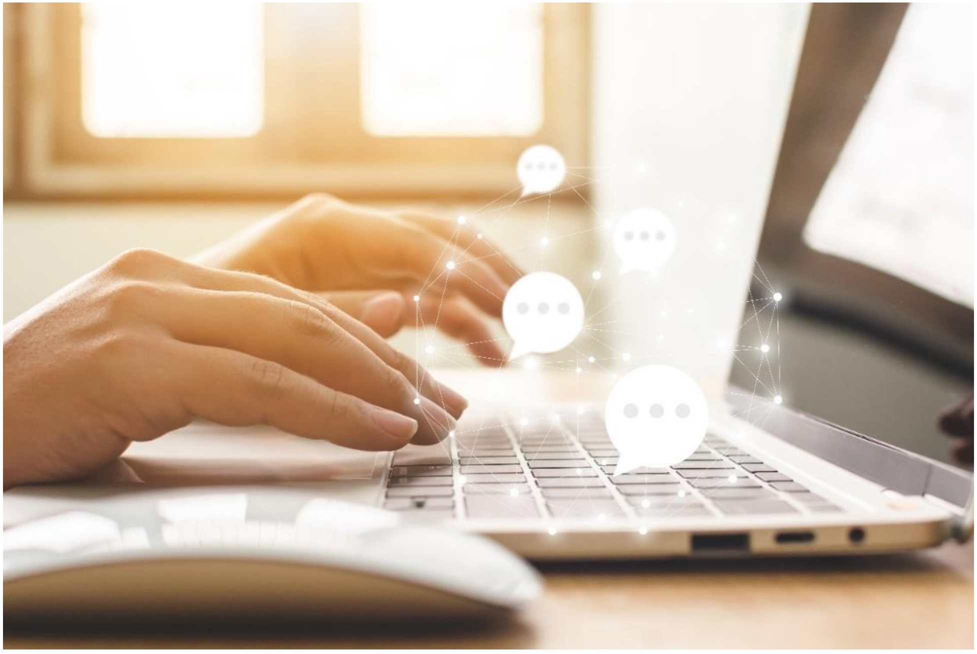
Associated fine objective: FO_01_03

Situation: Which measures can help you reduce the risk of online communication via e-mails?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Activate the file extension display (e.g. .docx, .exe).**
- Deactivate the file extension display.
- **Use appropriate security settings to prevent the execution of active content in e-mail programs.**
- **Scan suspicious attachments with a virus program.**
- Only disclose your user data if you know the companies who are asking for it very well.

2.Build knowledge - Forums and chat rooms

Forums and **chat rooms** are both well-known and popular media for online communication and information exchange, but they differ in the way they are used.



Definition
While chat rooms focus on communicating with people **in real time**, forums are more suitable for **discussions where not all participants need to be online at the same time**. Forums are also usually better organized, with discussions divided into threads that are moderated.

Chats and forums allow the exchange of text messages, but can usually also be used to exchange images, videos, links or files. Additionally, some chat rooms also support the use of microphones or webcams for chatting with other users.

In order to actively participate in forums and chats, a **registration with a valid e-mail address** is usually required. This is to prevent spam-posts, for example. Moreover, moderators also have the option of suspending or blocking users in forums or chats if they behave inappropriately. Nevertheless, the use of these communication media can result in various risks and threats, this include for example:

- **Maleware or links to phishing sites:** All files and links posted on forums should therefore be treated with caution.
- You should keep in mind that faking or hacking user accounts can mislead you into believing **false identities.**
- Communication in forums and chats is usually **completely unencrypted,** so your statements and written information can be read by every user. For professionals it is also no problem to read any private messages.

You don't want to do without forums and chats and are wondering what you can do to avoid security risks? The consideration of the following aspects is certainly an important step:

- Do not open files sent to you uncritically.
- Never pass on personal and sensitive data to persons you do not know personally.
- **Never allow anyone to access your computer**, not even within a chat session.

Example
You have a computer problem and are looking for advice in an expert chat. A supposed expert wants to help you. That's why you should give him control of your computer by remote control.

- You should **read the general terms and conditions** and the **data protection regulations of the communication service**, particularly with regard to what happens to your data and information. Are they sold, stored or encrypted?
- **Block contacts** if you're unsure who they are or if someone is harassing you. Report insults, sexual harassment, blackmail or threats to the police.
- Don't forget about **copyright:** you shouldn't send pictures or other files that you didn't create yourself without the permission of the author.
- Always **be cautious when dating a stranger** who you only know from forums or chats. Even if you have the impression that you already know the person, the information and statements provided by this person may all be fake or made up.

2.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_01

Situation: What are chat rooms and what do you understand by forums? How do the two communication tools differ from each other?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Chat rooms are very suitable for discussions in which not all participants have to be online at the same time.
- Forums are better suited for talking to others in real time than chat rooms.
- **Text messages can be exchanged in both chat rooms and forums. Often, you can also exchange pictures, video, links, or files.**
- **Chat rooms are better suited to communicate with others in real time than forums.**
- While you can also chat anonymously or under a pseudonym in chat rooms, it is necessary to disclose your real name in forums.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_02

Situation: Forums and chat rooms are very popular online communication tools. Nevertheless, which of the following risks can you face when using them?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **The infection of malicious software by opening files shared in chat rooms or forums.**

- **The redirection to phising sites by clicking in good faith on shared links.**
- That you suddenly incur very high costs by exchanging messages in forums.
- **That someone is trying to trick you into believing a fake or made-up identity.**
- **That your sent chat messages are also secretly read by third parties.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_0

Situation: Which of the following measures can you take to reduce the risk of online communication via forums and chat rooms?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Read the general terms and conditions of the communication service.**
- **Block contacts if you are unsure who they are.**
- Share only pictures or files that you did not design yourself.
- Only allow someone to access your computer if they have a trustable profile photo and username.
- **Do not open files sent to you uncritically.**

3. Build knowledge - Communication in social networks

In social networks, the assumption of presumed anonymity can lead to **thoughtless behaviour in dealing with data and information**. As a result, social networks are increasingly being targeted for fraudulent activities.

You should always **consider the following aspects** when dealing with social media:

- Never publish and discuss personal and confidential information in public virtual space. It can have legal consequences if you publish unconsidered and unprovable allegations.
- Every social network has the option of making personal information accessible only to certain categories of groups of people via filters. Check out these options so you never run the risk of having to welcome thousands of strangers to your private birthday party.
- You like to have as many friends as possible in social networks? Be careful not to forget the good old saying: "Show me your friends and I'll tell you who you are". **Accepting friends uncritically can have a negative effect on you** - e.g. if you are looking for a job. Many employers inform themselves about the activities of the applicants in social networks and use this information to make selection decisions in the application process.
- Always check social networking settings for privacy protection.
- Be aware that especially in social networks there is the **risk of deception**. Perpetrators deliberately deceive and manipulate their victims by providing them with misleading or potentially dangerous information.

Important
If you detect misuse or misconduct on social networks, you can and should report it to the service provider and appropriate authorities or organizations.

3.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_01

Situation: What should you consider when using social media to avoid possible negative consequences?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Accept as many friend requests as possible to make yourself appear as popular as possible to others.
- **Always check social media settings for privacy protection.**
- **Don't believe all the information you receive on social networks.**
- If you don't like someone and therefore would like to post very negative comments about him or her, be careful not to use your real name, especially if you use harsh language. This way you can remain anonymous and do not have to fear consequences.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_02

Situation: You're checking your social media account. In shock, you discover that someone has posted a video on the net showing a group of teenagers wildly bullying and abusing a girl both physically and physically. How should you react now?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **You should report it to the service provider (e.g. Facebook)**

- Unfortunately, there's nothing you can do. Maybe the video is not even real. To avoid being threatened yourself, you ignore it.
- You should report it to the police.
- You don't know the victim or the perpetrator, so you can't give anybody a concrete name. Therefore, there's no point in your interfering.

Sources

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/chat/

onlinesicherheit.gv.at:
https://www.onlinesicherheit.gv.at/gefahren_im_netz/soziale_medien/gefahren/250080.html

securitymetrics.com: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

ftc.gov: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

smallbusiness.com: https://smallbusiness.chron.com/differences-between-chat-rooms-forums-71296.html

socialnomics.net: https://socialnomics.net/2017/11/08/chatting-online-risks-the-tips-to-stay-safe/

getsafeonline.org: https://www.getsafeonline.org/social-networking/chatrooms/

cybersecurity.edu: https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/social-media

Save knowledge

Summary

The most popular form of online communication is **e-mail**, which is why **fake e-mails** are unfortunately quite common too. Fake e-mails are unwanted e-mails with maliciously false or misleading information. For example, **malware** is often hidden in the **attachments** of these fake e-mails.

In order not to fall for these fake e-mails, it is important to **stay alert.** For example, e-mails that promise you a big win or ask you to reveal confidential information should always be treated with caution. The same applies to emails with irritating words as subject matter such as "Your bank account has been blocked" or with an unusually high number of grammar or spelling mistakes.
Particular care should be taken with so-called **pishing mails**, where fake emails are used to try to obtain passwords. In order to reduce the risk of online communication, it makes sense to save suspicious e-mail attachments first and to **scan them with a virus program.**

There is also the risk of infecting your computer with malware or being forwarded to pishing sites by carelessly clicking on links or opening files when **communicating in forums or chat rooms**. False identities or unwanted co-reading of messages are further dangers that must be taken into account.
It is therefore particularly important **to read the data protection regulations** of online communication providers carefully and **never disclose personal or sensitive data** in chats or forums.

This also applies when using **social networks**. Be aware that especially in social networks there is the danger of being misled by false identities or by the conscious or unconscious dissemination of **false information**. If you detect misuse or misconduct on social networks, **you can and should report it** to the service provider and appropriate authorities or organizations.