2. Internet – Connecting ideas and people

> "Eventually everything connects – people, ideas, objects. The quality of the connections is the key to quality per se."
>
> *Charles Eames, early 20th century designer*

CHECKLIST FACT SHEET 6 – E-MAIL AND COMMUNICATION

Have you created several e-mail accounts and set different passwords for each?

Is the password sufficiently "strong" (more than 8 characters long, with a combination of letters, numbers and symbols)?

Do you clearly label your e-mails with relevant key words in the subject line?

Have you enabled two-factor security on your e-mail accounts (providing an extra security question and/or your mobile phone number)?

CHECKLIST FACT SHEET 7 – CHAT AND MESSAGING MEDIA

Have you included contact details in your website or blog?

Have you taken steps to protect your online privacy?

Have you checked that the content that you are using for your website/blog is in accordance with copyright law?

CHECKLIST FACT SHEET 8 – SOCIAL NETWORKING AND SOCIAL SHARING

Reputation is something we only have one of: do you systematically "think before you post"?

When did you last update your privacy settings on the sites you use?

Democracy depends on the participation of as many citizens as possible in the public debate: have you tried making your voice heard through relevant social network sites?

CHECKLIST FACT SHEET 9 – PRIVACY AND PRIVACY SETTINGS

Is it necessary to post that tagged photo on a social networking site?

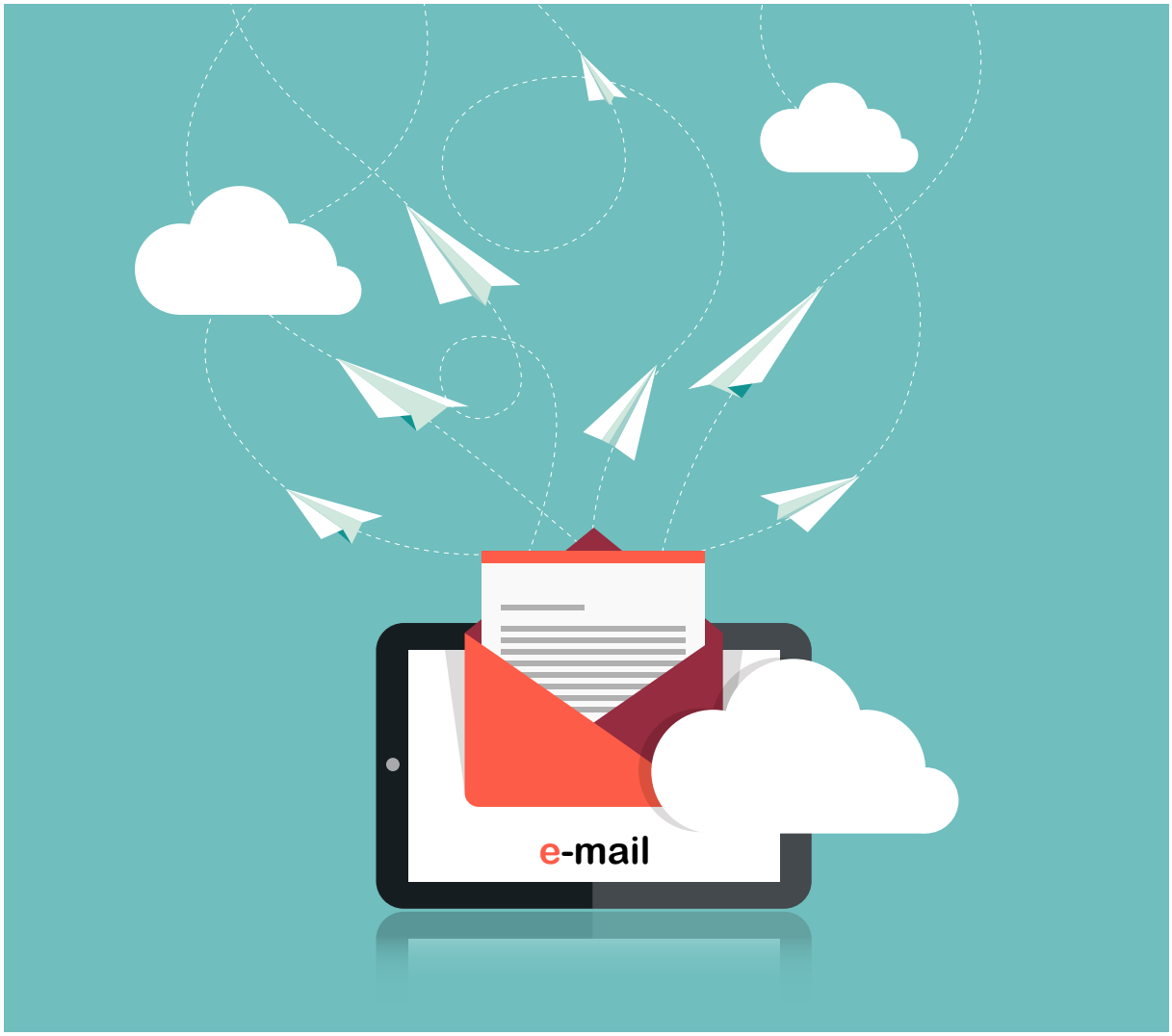
Have you read the mobile app agreement to understand what are you sharing: what you own and what "they" own?

When you upload apps, are you sure you know exactly what private information they will access? Is such access really necessary for the app to function?

Do you understand what the European Union's General Data Protection Regulation implies for you?

Fact sheet 6

E-mail and communication



E-mail[1], short for electronic mail, is the system for sending messages between computers connected in a network such as the Internet. The term also refers to the message itself. An e-mail is usually transferred successfully in a matter of seconds and the recipient can access and reply whenever it is convenient. A flexible and efficient system, e-mail has drastically changed the way we work and communicate. Billions of messages are sent every day.

An e-mail address is composed of two parts: local and domain names, separated by the "@" sign. The local name will often – but not always – indicate the name of a user. The domain may indicate the user's organisation, company or Internet service provider. Domain names may also indicate the type of organisation and/or country. For example, name@ox.ac.uk would be someone working or studying at Oxford University.

Although many other ways of communicating have emerged, e-mail accounts are still at the heart of a user's online experience since it is often the only way to create accounts to participate online. So, while other means of communicating may now be preferred to e-mails (social networking, instant messaging, etc.), e-mails have become the "key" to the online identity of users, serving often as a "login" to connect to all the online services they use.

1. https://en.wikipedia.org/wiki/Email

IMPORTANCE IN EDUCATION

Because e-mail addresses are so often asked for online, learning to manage an e-mail account properly carries a lot of educational value, much like learning to sort physical mail by classifying the personal content and the important administrative content in order to find it easily.

E-mail is also a valuable tool in cross-cultural projects between classes of children and young people in different countries. Children and young people can use it to develop their language skills and share information about their cultures.

Some of the more reserved children and young people may express themselves better through e-mail than they would in face-to-face classroom discussion.

ETHICAL CONSIDERATIONS AND RISKS

- Because your e-mail is the "gateway" to all your online accounts, the consequences of someone breaking into your e-mail account can be very serious.
- Most e-mail clients (computer programs used to access and manage a user's e-mail[2] you can find online are free, but many of them use algorithms to scan the content of your e-mails and display targeted advertising on the webmail page.
- The expression of emotions via e-mail is difficult. This is why you should always write your messages with care to make sure they are not misunderstood. "Emoticons"[3], small expressive icons such as smiley faces, can help you express your intentions, especially irony or humour. Use these sparingly, however, to keep from distracting from your message.
- A high proportion of e-mail received is unsolicited and usually undesired spam[4] (see Fact sheet 19 on spam, malware, fraud and security). Fortunately, spam filters are getting increasingly better at sorting spam from regular e-mails.
- Be sure not to contribute yourself to "spamming" by abusively forwarding e-mails that you find "funny" or "interesting" to all of your contacts. If you do so too often, spam filters may identify your e-mail address as a proxy for spam and blacklist it, making it impossible for you to contact anyone.
- Some "forwards" are false or fraudulent. An example are e-mails that falsely claim that a company or organisation has promised to pay a small sum of money for a humanitarian cause (often citing a cause such as a sick child requiring surgery) each time the mail is forwarded.
- It is easy to conceal a name in order to be misleading. This can be done by simply changing the name in the settings or creating a webmail address such as *elvispresley@hotmail.com*. Even if you recognise the e-mail address as belonging to one of your contacts, check the subject line too because it is possible that that the owner's machine may have become a "zombie computer"[5] affected by a hacker or virus.
- A link may appear to be directing you to one website when in fact it leads to another. This is particularly common in phishing scams[6].

2. https://en.wikipedia.org/wiki/Email_client
3. https://en.wikipedia.org/wiki/Emoticon#Basic_examples
4. https://en.wikipedia.org/wiki/Email_spam>
5. https://en.wikipedia.org/wiki/Zombie_(computer_science)
6. https://en.wikipedia.org/wiki/Phishing

GOOD PRACTICE

- Create several e-mail accounts for different purposes (signing up to social networking sites, purchasing products online, etc.). Keep one account as private as possible by not publishing it on the Web and using it solely for important services you and your friends use. Use a different one to sign up to services you might only use once, or services that you rarely use.
- Keep e-mail messages short and to the point. Try to avoid long blocks of text. Check your spelling.
- Make sure you include relevant words in the subject line. This helps the recipient identify your message as being genuine and helps to find the e-mail at a later time.
- Create strong passwords for your e-mail accounts (more than 8 characters long, combining letters, numbers and symbols) and use different passwords for each account.
- Be considerate in the volume of e-mail you send out and be smart and strategic about how you communicate with others. If you need to have a group discussion with a large number of people, perhaps it is more useful to organise a conference call or a chat on a private forum rather than sending a massive amount of e-mails.
- Avoid checking your e-mails every 10 minutes. Many people allow e-mail to be a constant interruption.
- As a general rule, never include sensitive information in an e-mail, such as bank details. There are only rare circumstances where you will need to send such information, for instance, to make a hotel reservation. In case of doubt, proceed with caution, check the online reputation of the service you want to use, check the procedure to cancel your card or the transaction, use more secure payment services, such as PayPal, and avoid less secure services, such as direct money transfer services (e.g. Western Union). However, never send details such as your username and password of your online accounts via e-mail. Online services will never ask you for this, so if you receive an e-mail asking for such details, it is definitely a phishing attempt.
- More and more sophisticated phishing strategies consist in "false" notification e-mails that emulate perfectly the messages you receive from the services you use (social networking sites) and send you to a false website that asks for your username and password to log in. Make sure that you always check the e-mail address of the sender and the address of the website for anything unusual.
- Maintain a healthy scepticism about e-mails you receive. Do not open e-mails if you do not trust the source.
- Be especially wary of attachments. If you were not expecting an attachment from the sender or do not trust it for any other reason, delete without opening. Even attachments from known and trusted senders should be first saved then scanned before opening.
- Make use of all the security features that your e-mail client proposes. Usually, e-mail clients enable you to enter a secondary email address in case that e-mail account gets hacked and, increasingly, e-mail clients propose that you enter your mobile phone number for extra security checks in exceptional circumstances. If your account is compromised, configure your security settings properly so it will be much easier for you to recover it.
- Be sure to consult Fact sheet 19 on spam, malware, fraud and security for additional advice on e-mail.

HOW TO

- To consult your e-mails, you can either use the "official" app of the e-mail service on your smart-phone, tablet or even your computer running Windows 8 or above (such as the Gmail app, the Outlook app or the Yahoo! app), you can go to the website of the e-mail service (using a "web-

mail" service) or you can use an email client which is an external application that downloads your e-mails from your e-mail service and enables you to manage/organise them. The "up" side of using an e-mail client is that you can configure it to download e-mails from several different e-mail services so you can consult all of your e-mails from your different e-mail addresses in one place. The most popular e-mail clients are Thunderbird and Outlook. E-mail clients are mostly used for professional e-mail.

- For information on setting up a spam filter see Fact sheet 19 on spam, malware, fraud and security.

IDEAS FOR CLASSROOM WORK

- For older students that have an e-mail address, ask them to connect to their e-mail service and explore the security settings in order to secure their e-mail account by adding an additional security question, a second e-mail or a mobile phone number.
- Here are the procedures to follow to secure your e-mail account for Gmail, Yahoo! and Outlook.
  - ▶ *<https://support.google.com/accounts/answer/46526?hl=en>*
  - ▶ *<http://windows.microsoft.com/en-us/windows/outlook-security>*
  - ▶ *<https://help.yahoo.com/kb/SLN8292.html>*
- There are many e-mail providers out there besides the three "big" ones above. Why insist on those three? Because, at least for Gmail and Outlook/Hotmail, they are linked to many other services. For instance, a "Google" account is almost a necessity when you own an Android smartphone and an Outlook account is often linked to your Windows operating system. This means that, regardless of your preferences, you might be "forced" to create an e-mail account on one of the services above. But you are of course free to use e-mail clients with higher privacy standards such as Web.de or Protonmail.com. Even your Internet service provider usually offers an e-mail service. Feel free to search for other alternatives online.
- Get your students to work in teams of three or more and ask them to make up good passwords for an imaginary e-mail account. Be very clear that they should not share their real password! After a 10-minute brainstorming, ask each team to present their proposed password and why they think it is secure. Help them identify the characteristics of a strong password (more than 8 characters long, combining letters, numbers and symbol characters) and the common pitfalls of weak passwords (can be found in a dictionary, is related to you in some way – name of dog, family name, etc.).

FURTHER INFORMATION

- Well-known examples of e-mail clients are Microsoft Outlook *<https://products.office.com/en-us/outlook/email-and-calendar-software-microsoft-outlook>* or Mozilla Thunderbird *<http://www.mozilla.org/projects/thunderbird/>*.
- Truth or Fiction is a website for Internet users to check the veracity of commonly forwarded e-mails *<http://www.truthorfiction.com/>*. Another similar website is *<http://m.snopes.com/whats-new/>*.
- Three of the most popular webmail sites are Outlook *<https://office.live.com/start/Outlook.aspx>*, Yahoo! *<https://mail.yahoo.com>* and Google's Gmail *<http://www.gmail.com>*. Feel free to search for alternative e-mail providers, especially in your country.
- Relevant UN Convention on the Rights of the Child articles:

  Article 13 – Children have the right to get and to share information as long as the information is not damaging to them or to others.

  Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.