DIGITAL ACCESS

DIGITAL SKILLS FOR PEOPLE LIVING IN THE 3RD AGE
Effective Digital Access to Public Services

Erasmus+

DIGITAL ACCESS PROJECT

LEARNING MODULE

Basic online safety knowledge

Prepared by: AKLUB

September 2018

This project has been funded with support from the European Commission. This publication 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.

Contents

LEARNING HOURS: [ALL UNITS LEARNING HOURS]

WORKLOAD: [ALL UNITS LEARNING HOURS + OVERALL TIME FOR THE EXERCISES]

SUMMARY

This module designed to learn basic user's knowledge of online safety for novice user of the internet. The unit's primary objectives is to learn the user how to keep personal information safe ensuring their online data and assets are not compromised.

KEYWORDS

Online safety, Personal information, Password, Cyberstalking, Password vault

MODULE OBJECTIVES

Actions / Achievements		
Acquiring an understanding of internet based criminal activities targeted at individuals and the acquisition of the skills to identify and avoid these activities.		
Knowledge	**Skills**	**Competencies**
Online safety	Understanding Online safety Understanding types of online risks Understanding of basic keywords	Understanding why is online safety important and what are online risks.
Personal information	What is my personal information Disclosing personal information online What might happen if I share my personal information online How can I protect my personal information	Being able to understand what are personal data, what are the risks in online environment and be able to protect your personal data.

Passwords	Choosing the best password Looking after your passwords Actions to be taken to protect your self	Understanding of the importance having strong passwords. Create and manage passwords and user accounts.
Privacy settings	Identifying cyberstalking Coping strategies Using password vaults Managing user accounts	Understanding of the importance having strong passwords. Create and manage passwords and user accounts.

UNIT 1: Online safety

Outcome

Understanding why is online safety important and what are online risks.

Introduction

10 basic online safety rules

1. Keep Personal Information Professional and Limited

Nobody don't need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn't hand purely personal information out to strangers individually—don't hand it out to millions of people online.

2. Keep Your Privacy Settings On

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of your information. Both web browsers and mobile operating systems have settings available to protect your privacy online. Major Websites like Facebook also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

3. Practice Safe Browsing

You wouldn't choose to walk through a dangerous neighbourhood—don't visit dangerous neighbourhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you don't even give the hackers a chance.

4. Make Sure Your Internet Connection is Secure

When you go online in a public place, for example by using a public Wi-Fi connection, you have no direct control over its security. Corporate cybersecurity experts worry about "endpoints"—the places where a private network connects to the outside world. Your vulnerable endpoint is your local Internet connection. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before providing information such as your bank account number. You will learn more about in intermediate module.

5. Be Careful What You Download

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. Don't download apps that look suspicious or come from a site you don't trust.

6. Choose Strong Passwords

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters. We will talk about this later in this lesson.

7. Make Online Purchases from Secure Sites

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. As you can identify secure sites by looking for an address that starts with *https:* (the S stands for *secure*) rather than simply *http:* They may also be marked by a padlock icon next to the address bar.

8. Be Careful What You Post

The Internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original (say, from Twitter) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made. Don't put anything online that you wouldn't want your relatives or other people to see.

9. Be Careful Who You Meet Online

People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to catch up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

10. Keep Your Antivirus Program Up To Date

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

Keep these 10 basic Internet safety rules in mind and you'll avoid many of the nasty surprises that lurk online for the careless. In next lessons and modules we will go to more detail to teach you how to apply those rules into practice.

UNIT 2: Personal information

Outcome

Being able to understand what are personal data, what are the risks in online environment are and being able to protect your personal data.

What is my personal information?

Your personal information may include your:

Full name
Address
Phone numbers
School
Date of birth
Email address
Username and password
Bank and credit card details.

Disclosing personal information online

Many online services require users to provide some personal information in order to use their service. Prior to providing personal information, you should think about what can be done with your personal information and assess whether you are still happy to pass on these details. In addition to inappropriate or illegal use of information, disclosing personal information online can impact your digital reputation.
There are several online activities that you should be aware of that may require a level of disclosure of personal information. These include:

Shopping: to verify the identity of the purchaser, to process payments or for the delivery of goods.

Subscribing or registering: a screen name or ID and an email address are often minimum requirements but other requested information may include: age, gender, address, photo and personal likes or dislikes (a red asterisk (*) generally identifies mandatory fields that are needed to register).

Competitions, prizes and rewards: often require users to provide extensive personal data, including personal interests and demographic details—these are often used by marketers to promote products and services.

Online games and virtual worlds: these may require users to register before they can begin to play.

What might happen if I share my personal information online?

Spam, scams, identity theft and fraud are just some of the more serious issues that you might face if you are sharing personal information online.

How can I protect my personal information

It's important to understand how personal information is used online and how to protect your information and digital reputation.

The following tips are a great basis for protecting your personal information online:

Only disclose financial information on secure websites. Look for an address beginning with https:// and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.

If in doubt about the legitimacy of a website, call the organisation it claims to represent. The SCAMwatch website provides further advice on how to identify and report potential scams.

Banking institutions will never email individuals asking for their user name or password. If you receive an email by an organisation claiming to represent a banking institution report the email to the bank and SCAMwatch. Do not respond and do not click on any links provided.

Read user agreements and privacy policies. Many organisations use information for marketing purposes and may sell it to other marketing firms. If information is posted on websites that do sell information to marketers, individuals may receive promotional spam emails which can be difficult to stop.

Reduce spam by protecting your details. Spam can be reduced by:

limiting disclosure of email addresses and mobile numbers

installing and using spam filtering software

checking the terms and conditions when purchasing products, entering competitions or registering for services or email newsletters

not allowing contact details to be used for marketing purposes (making sure you check the opt out box)

boosting online security to limit spam.

Understand that information shared online can be permanent—users may not have control over who sees or accesses their personal information.

Select passwords carefully. When creating passwords there are some definite dos and don'ts, these include:

Do

use eight characters or more

use a combination of words that aren't predictable

use two-factor authentication on accounts containing personal information.

Don't

use pet names, birthdates, family or friends' names

use a predictable combination of words (eg. 'ilovehiking'), a context specific word (eg. 'google') or repeated sequential characters (eg. 'aaaaaa' or '123456')

share passwords with others, even with friends

store them on your device, unless it's via a password manager which stores them in an encrypted database.hreat and extortion scams include 'ransomware', 'malware' and 'hit man' scams. Ransomware and malware scams can involve harmful software being placed on your computer. This can give criminals access to your personal information, which may result in loss of data or prevent you from accessing your programs and files. Scammers then demand payment before allowing you to access your computer again.

UNIT 3: Passwords

Outcome

Identifying and dealing with cyberstalking and the avenues to report it.

Introduction

Your passwords are the most common way to prove your identity when using websites, email accounts and your computer itself (via User Accounts). The use of strong passwords is therefore essential in order to protect your security and identity. The best security in the world is useless if a malicious person has a legitimate user name and password.

Passwords are commonly used in conjunction with your username. However, on secure sites they may also be used alongside other methods of identification such as a separate PIN and/or memorable information. In some cases you will also be asked to enter only certain characters of your password, for additional security.

The Risk of Using Weak Passwords and not Having a Separate Password for Your email Account

People impersonating you to commit fraud and other crimes, including:
- Accessing your bank account
- Purchasing items online with your money
- Impersonating you on social networking and dating sites
- Sending emails in your name
- Accessing the private information held on your computer

Choosing the Best Passwords

Do:

Always use a password.

Use a strong, separate password for your email account.

To create a strong password, simply choose three random words. Numbers, symbols and combinations of upper and lower case can be used if you feel you need to create a stronger password, or the account you are creating a password for requires more than just letters.

There are alternatives, with no hard and fast rules, but you could consider the following suggestions:

Choose a password with at least eight characters (more if you can, as longer passwords are

harder for criminals to guess or break), a combination of upper and lower case letters, numbers and keyboard symbols such as @ # $ % ^ & * ( ) _ +. (for example SP1D3Rm@n – a variation of spiderman, with letters, numbers, upper and lower case). However, be aware that some of these punctuation marks may be difficult to enter on foreign keyboards. Also remember that changing letters to numbers (for example E to 3 and i to 1) are techniques well-known to criminals.

A line of a song that other people would not associate with you.

Someone else's mother's maiden name (not your own mother's maiden name).

Pick a phrase known to you, for example 'Tramps like us, baby we were born to run'" and take the first character from each word to get 'tlu,bwwbtr'

Don't:

Use the following as passwords:

Your username, actual name or business name.

Family members' or pets' names.

Your or family birthdays.

Favourite football or F1 team or other words easy to work out with a little background knowledge.

The word 'password'.

Numerical sequences.

A single commonplace dictionary word, which could be cracked by common hacking programs.

When choosing numerical passcodes or PINs, do not use ascending or descending numbers (for example 4321 or 12345), duplicated numbers (such as 1111) or easily recognisable keypad patterns (such as 14789 or 2580).

Looking After Your Passwords

Never disclose your passwords to anyone else. If you think that someone else knows your password, change it immediately.

Don't enter your password when others can see what you are typing.

The routine changing of passwords is not recommended, unless the accounts to which they apply have been hacked, in which case they should be changed immediately. This also applies if another account or website for which you use the same login details have been hacked.

Use a different password for every website. If you have only one password, a criminal simply has to break it to gain access to everything.

Don't recycle passwords (for example password2, password3).

If you must write passwords down in order to remember them, encrypt them in a way that is familiar to you but makes them indecipherable by others.

An alternative to writing down passwords is to use an online password vault or safe. Seek recommendations, and ensure the one you choose is secure and reputable.

Do not send your password by email.

The fact that you should use different passwords for each of your accounts can make them very difficult to remember. Consider using one of the many password vaults available on the internet, but read reviews and get recommendations.

Password Vaults/Safes

There are a number of password vaults (otherwise known as password safes or perhaps another term) available for your use - some paid for, some free of charge. These enable you to store all of your passwords in one, easy-to-access location so that you do not need to remember them all, or write them down. You merely need to remember one set of login details.

You should read reviews or get personal recommendations before entering your passwords into a password vault. Whichever you choose, our recommendation is that it features two-factor authentication (2FA) - in other words, it sends a code to your mobile phone or other device, which you need to enter into the password vault in order to gain access, much like when you confirm an online bank payment.

Controlling User Accounts

Everybody who uses a computer should be assigned their own user account so that only they can access their files and programs. Each user account should be accessible only by entering a username and password in order to safeguard users' privacy.

Do not use an account with administrator privileges for everyday use, as malware could assume administrator rights. Even if you are the only user, set up an administrator account to use when you need to carry out tasks such as installing programs or changing the system configuration, and another 'standard user' account as your regular account. If you are not logged in as administrator, you will be prompted to enter an administrator password when you install a new device driver or program.

UNIT 4: Privacy settings

Outcome

Helping a user to identify, deal with and report cyberbullying.

Computer Privacy

Take a look at the privacy settings offered in your browser (usually found in the Tools menu) to see whether you can fine-tune them to keep the good and block the bad. When you go online, websites install cookies on your computer that track your movements. Some cookies can be beneficial, such as those that remember your login names or items in your online shopping cart. But some cookies are designed to remember everything you do online, build a profile of your personal information and habits, and sell that information to advertisers and other companies.

Internet Explorer setting example

To protect your computer from intrusion or from viruses that could corrupt your system, you need to know how to change the privacy settings in Internet Explorer. By changing the privacy settings, you decide what kinds of sites Internet Explorer can access and what kinds of sites you want to protect your computer against.

1. Open Internet Explorer, choose Tools→Internet Options, and click the Privacy tab.

2. Drag the slider up and down to see the different levels of security settings.

At each level, Internet Explorer will give you information about that specific security setting.

3. Read the choices and select a setting that suits you.

If you don't know what to choose, Medium is a good place to start. If that doesn't seem to block enough, you can always increase the security level.

4. Click the Sites button to specify sites that should always or never be allowed to use cookies.

The Per Site Privacy Actions dialog box opens, letting you override the general setting you chose with the slider.

Enter a site in the Address of Website box and click either Block or Allow.

Click Allow for sites you know you can always trust, and click Block for sites you know you can never trust (like www.ComputerDemolishingDownloads.com).

5. Click OK to save your new settings.

You return to the Internet Options dialog box.

6. Adjust your pop-up blocker and click OK when you're done.

You can turn the pop-up blocker on and off from here, and you can allow certain Web sites' pop-ups through the blocker by clicking the Settings button. You add sites here the same way you added sites in the Per Site Privacy Actions dialog box.

Smartphone Privacy

Settings on smartphones vary, but you can tighten up privacy with these precautions:

Turn off location services. That prevents apps from tracking your location.

Don't let apps share data. Some apps want to use information stored on your phone (your contact list, for example). Say no.

Enable privacy settings on apps you download. Make sure you are using strict privacy settings on services such as Instagram and Facebook.

Be careful with social logins. When you log onto a site with your Facebook or Google username and password, you may be allowing that app to access certain information from your profile. Read the fine print to know what you're sharing.

EXERCISES

What is your Privacy IQ? Take our quiz and find out!

https://blog.avast.com/2014/01/27/what-is-your-privacy-iq-take-our-quiz-and-find-out-2/

Online game for cybersecurity

NOVA has joined forces with cybersecurity experts to create its Cybersecurity Lab. This is a game where players discover how they can keep their digital lives safe. The game helps players develop an understanding of the common cyber threats that exist online and their defences.

https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Worst passwords list

FURTHER READING AND RESOURCES

Terms that you should know

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Internet Safety planning for seniors (PDF download)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjAReqQIBxAC&url=https%3A%2F%2Fvictimserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSeniors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Internet safety rules

https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

How to stay safe online for seniors –Youtube video

https://www.youtube.com/watch?v=HGHxRNT6PjU

Online safety for seniors

https://www.connectsafely.org/seniors/

More online safety info

https://www.protectseniorsonline.com/resources/