Project IDCAP: Improve Digital Competence in Adult People

Project Number: 2018-1-PL01-KA204-051003

Digital Identity

Introduction 3

1. Management of digital identity 4
2. Management of internet account 5
3. Security issues and privacy 6
4. Digital footprint 7
5. Online identity 8

Summary 10

Bibliography: 11

Introduction

In terms of digital or internet based identity digital identity is the information which represents real person or other external agent. External agent might also be a single machine, system and/or application. ISO/IEC 24760-1 defines identity as "set of attributes related to an entity”[1]. Nowadays we speak about identity as particular attributes to an entity which has replaced the term “agent”. In this document we will be referring to digital identity only as the identity of a physical person.

Here we will present the basics of management of your digital identity and why it is important to protect it. Next we will see in more details how to manage and internet account and what are the key steps in the process. Further on, we will present the basics for security and privacy online. Finally we will briefly discuss about digital footprint and online identity issues.

[1] ISO/IEC 24760-1: A framework for identity management - Part 1: Terminology and concepts". ISO. 2011.

1. Management of digital identity

Management of digital identity relays on principles which follow more or less well known mechanisms which were developed for non-digital identity. Although it might seem complicated think about your ID card. When asking to receive your ID card, the authority issuing it validates from other authorities your birthday, tax number, citizen number (where applicable), take a new photo of you etc. In the digital world your digital identity may be as simple as your username and password or it can have many more levels of complexity, which are there to guarantee that the owner of that particular identity is you, and only you. These levels may include a separate e-signature, token for "random" generation of particular digital code, SMS confirmation or code being send to particular mobile phone (which is known to be registered to specific person), voice identification, answer of particular question (like What was your first pet name?), fingerprint validation and many other. All those levels are in place to guarantee that only the specific person is authorized to perform some actions in the digital world.

Many people find those levels difficult to understand, confusing and frustrating. They might be right but on the other hand one should understand that the digital world is a direct representation of the physical world and no one would like their "digital" money to flow away from their "real" bank account. Institutions and especially banks place various levels of security not to annoy the users, but to protect their identity and to ensure right of operations and transactions. In parallel more and more services are offered through your mobile phone. These cover so wide range that we will list here just few as illustration. Think of them as services that directly influence your "real" bank account. Some of those services done via smart phones (depending of your country of residence) may be:

- Payment of parking via SMS message
- Payment of your bill at the supermarket

- Payment of your house bills
- Direct money transfer through dedicated bank authorized application

3D authenticated payment of your VISA or Master Card – after you have submitted the card number, validity and security code, this system sends SMS with 6 digits code to verified in advance mobile phone, which will add one more layer of protection of your card transactions.

Tickets for land transportation and boarding passes for airplanes
With "Apple pay" and "Google Wallet" your mobile phone becomes a wallet for any payment that supports NFC or magnetic payments. It even allows you to receive payments from various internet based sites, stores and users.

It is understandable why it is so important to properly manage your digital identity and why one needs to protect it vigorously

2. Management of internet account

As a part of your digital identity your internet based account is a first and in many cases not avoidable step. It is usually connected to email service like Googe's Gmail, Yahoo mail, Microsoft email, etc. Once you have created such account you have at least two variables attached to it: your user name and your password. Today most of the provides require a mobile phone number to be attached and verified to each specific account. Thus you have 3 attributes to a digital identity account – your username, your password and your mobile phone number. In many cases this verification without asking you and in order to further protect you adds not only the phone number but also the unique mobile phone production number called IMEI – International Mobile Equipment Identity. This number, which is assigned during manufacturing, is required to authorize mobile phone use over a mobile network too. That information is encrypted and kept safe by the internet service providers, but still in some rare cases can be stolen or misused (like in the case of Facebook and Cambridge Analytica, where millions of users ‘ data have been given to a company in order to do targeted advertisement for a political purposes). Here are some tips to help you with your digital identity:

Username: chose username that is clearly representing you. Think that you might be using this particular email address in the future and funny names are not always well accepted. Your username will stand before the @ sign of your email so names like easygirl@, toughguy@, yournightmare@ are not only to be avoided but you should avoid them at all. When choosing your username do not include numbers like your birthday or your loved ones’ birthdays.

Password: Use a combination of small letters, Capital letters, numbers and special characters like #,$,&,|, ~. Make it at least 8 characters and in change your password frequently. If you are accessing your digital account through your mobile phone use fingerprint or other form of authentication. Do not “remember” your account password at your browser.
Even if not required explicitly add your mobile phone to your account and set it as the default device to recover any forgotten passwords. Look into the settings of your account and set recovery email and phone number to authenticate your identity even better. Do not use the same password to other accounts like those on social networks or games.

3. Security issues and privacy

Some servers and applications can gather extensive information about particular use and it can potentially be linked to the physical person and his/her digital habits over internet. At EU level the GDPR (General Data Protection Regulation) is trying to deal with this, but still users are high advised to be careful what and where they share and do over internet and especially some social networks.

To process your digital content there are numerous editors for both photo and video, while usually social media provide spell checking capabilities for written text in English language too. On digital photos (and videos) you can add different filters, change saturation, contrast etc.. You can use the ones provided with your device or install the one you like most. Keep in mind that most of the online free editors usually have some limitations and you have to buy one to unlock all features. Those software services often add to your photo or video written sign that the material has been created using this software, which you may not like. Experiment and check till you find the one that satisfies your needs.

4. Digital footprint

Digital footprint refers to the unique traceable digital activities of a particular user on internet. The term can also be found as digital shadow, internet footprint, cyber shadow etc. Although usually the term is applied to physical persons it can also be used for organizations, companies, corporation, digital services sites etc. There are two types of digital footprint – active and passive.

Passive digital footprint – this term refers to data collected without the knowledge of the person. It may not necessarily be hidden by the user. Active digital footprint is the one that the user deliberately shares about themselves usually on social media or various websites. Information about the user may be intentionally or unintentionally left and then this information is actively or passively collected by other parties. For example if in your social media profile you have left visible to all your email address, your mobile phone number, your address of living, your workplace, internet address of your company etc. it will be relatively very easy for computer program or physical person to collect very big amount of information for you. In some cases this information may also include your bank accounts or tax records if breach in security records occurs.

There have been a number of studies that show that roughly 70% of all digital behavior of people is conscious and accountable for. However, about 30% of every persons' digital footprint may be in a form one would have never intentionally disclosed to the public. That leaves quite a lot of data for analyses of buying behavior, online purchase habits, hobbyies and other areas of personal life. While there is nothing wrong in clients analyses on large databases when triggered to individuals such analyses may be the foundation for identity theft, criminal activities and privacy breaches.

While digital foot print is not digital identity or digital ID the content and the descriptive data (also called meta data) impact strongly on privacy, internet trust and digital reputation. Internet footprints can be used by companies when recruiting new personnel, law enforcement agencies when collecting data on specific individuals cannot be collected in other means, marketers - they are searching what type of products the user(s) is/are interested in or to raise interest of users in specific product or service. Social networks are the primary source of such information. In some cases the social platforms may collect data from the user's device, even without the user knowing it, using various sensors on the mobile phones or other devices of the user. For example Facebook and Google collect extensive amounts of user information which if combined together can describe quite in details the user's personality, interests, political views, buying habits and interests etc.

5. Online identity

Online identity is the identity the user choses to build on internet, usually for gaming purposes. Users can choose to represent themselves with avatars (icon sized graphic) rather than with their real photos. Users can also use pseudonyms instead of their real names. An online identity may even be determined by user's links to internet group of people. Online identities are associated with real users through authorization procedures like registration and logging-in (username and password), as well as through specific IP address of a machine or device. Such sites often install tracking cookies that can further on determine the user's online behavior and link it to real person. As gaming is often, but not always, targeted to younger audience which is not so careful in protecting themselves online, it is crucial that the notion of digital identity, online identity and digital footprint be made as clear as possible to everyone using internet.

Summary

We have introduced the basic concepts and knowledge about management of digital identity and internet account. Following those key concepts we have described what are the security issues and user privacy. Finally we have introduced what is digital footprint and online identity.

Bibliography:

- https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/
- https://www.forbes.com/sites/forbestechcouncil/2019/06/07/a-beginners-guide-to-online-privacy-12-important-tips/#5092374e53ed
- https://assets.mozilla.net/pdf/IHPbriefs_Online_Privacy_March_2017.pdf
- https://www.commonsense.org/education/digital-citizenship/topic/digital-footprint-and-identity