Digital Literacy and Electronic Business

encyclopedia

MDPI

Entry

Digital Literacy and Electronic Business

Paul Grefen [1,2]

[1] Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands; p.w.p.j.grefen@tue.nl
[2] Atos Digital Transformation Consulting, Flight Forum 3000, 5657 EW Eindhoven, The Netherlands

Abstract: DefinitionDigital literacy is a term that traditionally describes the extent to which a person is able to use interactive digital devices for living and working, such as computers and smartphones, as well as services delivered through these devices. The advent of the digital society at large and electronic business, specifically in the past decades, has broadened the use of digital devices beyond the isolated uses of working and simple communication; this advent has created digital ecosystems in which workers and consumers are embedded to various degrees, such as social media platforms or integrated shopping and media platforms. This embedding implies that a traditional, narrow notion of digital literacy needs to be extended and made more precise. For this purpose, we use the related notions of *digital dexterity*, *digital proficiency* and *digital awareness*. The term *digital dexterity* describes the extent to which an individual can handle or operate digital devices or services from a physical perspective. The term *digital proficiency* describes the extent to which an individual can use digital means to effectively and efficiently facilitate their living and working. The term *digital awareness* describes the extent to which individuals can understand what their position in digital ecosystems is, including the opportunities and threats of participating in these ecosystems. *Digital literacy* in the modern, broad interpretation is then the combination of digital dexterity, digital proficiency and digital awareness.

Keywords: digital literacy; digital dexterity; digital proficiency; digital awareness; electronic commerce; digital ecosystem; online platform; consumer behavior; privacy; security; lock-in

Citation: Grefen, P. Digital Literacy and Electronic Business. *Encyclopedia* **2021**, *1*, 934–941. https://doi.org/10.3390/encyclopedia1030071

Academic Editors: Chia-Lin Chang, Michael McAleer and Philip Hans Franses

Received: 15 June 2021
Accepted: 2 September 2021
Published: 7 September 2021

1. History of the Digital Society and Digital Literacy

The practical use of computers and related digital technology started somewhere in the middle of the 20th century. This practical use was first confined to government organizations and large business institutes; computers were very large, very complicated, and extremely expensive. Consequently, operation of computers was performed by only a small group of professionally skilled employees of these organizations. To all other people, computers were large machines inside large buildings not so much different from other large machines, often of a more mechanical kind, that one need not understand, let alone be able to operate.

With the personal computer becoming popular in the 80s of the 20th century [1], this situation started to change; the use of computing facilities came into the reach of the general public. In the early years of this development, this use was, however, limited to very specific applications for a rather limited group of individuals: those with a strong interest in digital developments. The use of computers in business environments was still largely limited to specially qualified staff. Hence, the ability of the general public to operate computers was not seen as a major societal issue. Apart from formal courses in higher education, computer training for the general public was often limited to hobby-like classes for those really interested.

At the end of the 20th century, this development changed profoundly through the advent of large digital infrastructures. The Internet had been growing exponentially and continued to do so [2]. In its 'bare' form not so usable for the general public, the Internet

provides the basis for other digital infrastructures. Between 1995 and 2005, we see the emergence of the World Wide Web as such an infrastructure built on top of the Internet. The World Wide Web made its way into modern society on a large scale and is therefore nowadays in everyday speak simply referred to as 'the Web' or–incorrectly–'the Internet'.

The Web makes internet resources easily available through pages in natural language that are linked to allow easy navigation between these pages. Initially mainly used for displaying mostly textual information in a rather static way, the Web was quickly extended with features that allow much more interactive use and presentation of diverse media. This was the basis for the start of electronic commerce (e-commerce in short) on the Web. Starting around 1995 with a few web shops of some tech-savvy companies, around the turn of the century we see that many commercial organizations embrace the Web as a main interaction channel for their business activities. Not long after, we also see non-commercial organizations venturing onto the Web for interaction with their members or customers, for example in the domain of electronic government. Consequently, electronic commerce evolved into a more general form of electronic business (e-business in short). Electronic business is the kind of business that is enabled by the use of information technology (IT); not only supported by IT [2]. In other words, the use of IT is essential for interacting with customers in e-business. In this context, digital channels become mainstream in value delivery, influencing business strategy [3]—both in the business-to-business (B2B) domain [2,4] and in the business-to-consumer (B2C) domain [2]. In this era, lack of digital literacy started to become a small issue; without the knowledge of how to use digital devices, one could not use digital services. Usually, however, non-digital alternatives were broadly available.

Roughly between 2010 and 2015, we see that digital channels start to become the default means of interaction between organizations and individuals in a number of domains. Shopping on the Web starts to become an important alternative to physical shopping in traditional stores. Electronic banking becomes more and more attractive, based on extending customer-oriented functionality. Digital communication like email starts to replace physical communication like traditional post at an increasing pace. The rise of the smartphone [5] heavily contributes to this rise of digital interaction with an anywhere, anytime character. This development makes digital literacy more and more of an issue; a lack of digital literacy implies the inability to use modern channels for interaction in society and business. This also makes digital literacy a complex concept; it is not only about handling digital devices, but also about properly interacting in new digital settings.

In recent years, we see that the spread of digital interaction takes place so widely that it starts to negatively influence the availability of channels for non-digital interaction. A typical business-oriented example in many countries is the advent of electronic banking. With more and more people having access to digital channels and obvious efficiency advantages for banks in interacting electronically, we see a decrease in the availability of traditional banking; customers increasingly prefer mobile devices as their "branch" [6] and consequently many banks are closing many of their smaller local branches. On top of this, customers can be charged extra fees for the use of physical channels, such as traditional post to deliver account statements, to compensate banks for the lesser efficiency of such channels. In this setting, digital literacy starts becoming a real issue in society at large; a lack of digital literacy may make important societal and business functions very hard or even impossible to use.

Next to the rise of new possibilities through digital channels, we also observe the rise of new threats. There is the well-known threat of cyber-crime, in which criminals use digital channels to perform criminal acts [7]. Other threats may be less obvious to many individuals, however. An example is the threat to the privacy of individuals or the threat of consumer lock-in by large digital platforms. This requires the notion of digital literacy to be interpreted in a broader sense, as explained in the next section.

2. Extended Model of Digital Literacy

Currently, there is no generally accepted definition of digital literacy; definitions differ between contexts, such as countries [8]. The complex nature of the concept allows for various interpretations. A neutral definition was provided by UNESCO in 2018 [8]:

> *"Digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy and media literacy."*

In the same report, UNESCO uses the DigComp framework [8] as a framework for organizing competence areas and competences for individuals (referred to as 'citizens' in DigComp) that are part of digital literacy. This framework lists five competence areas, each covering three to six competences. The competence areas of DigComp 2.0 are [8,9]:

1. Information and data literacy
2. Communication and collaboration
3. Digital content creation
4. Safety
5. Problem solving

In this paper, we do not concentrate on specific competence areas or competences. On the one hand, these competences are too specific for this paper. On the other hand, competence frameworks like DigComp may evolve over time, based on the introduction of new digital technologies or new interaction patterns in society or business. Note for illustration of this point that DigComp contains competences that were simply irrelevant in earlier time frames, like "2.6: Managing digital identity" [8,9].

We use a simple model for the notion of extended digital literacy, consisting of three main components (as illustrated in Figure 1):

1. *Digital dexterity* describes the level to which an individual can handle or operate digital devices or services from a physical perspective; it refers to physical skills without a specific goal direction.
2. *Digital proficiency* describes the level to which an individual can use digital devices or services in an effective and efficient way to reach specific goals (either of the personal, social or business kind); it brings reasons to use one's digital dexterity.
3. *Digital awareness* describes the level to which an individual can understand the context and consequences of using digital devices or services (either of personal, social or business kinds); it generally contextualizes digital proficiency.

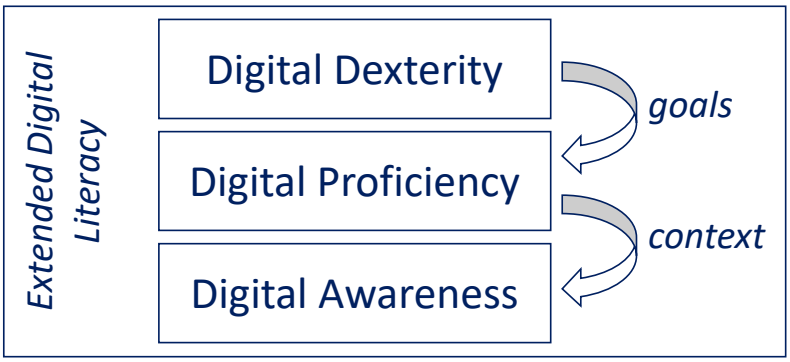

Figure 1. Components of extended digital literacy.

In the three following sections, we pay attention to these three components of extended digital literacy and place them in a contemporary context that explicitly includes electronic business.

3. Digital Dexterity

The level of digital dexterity of an individual determines to what extent that individual is able to physically operate digital devices and services offered through these devices. This notion is different from the notion of the digital dexterity of an organization [10]. Without an adequate level of digital dexterity, an individual cannot reach any level of autonomous digital proficiency. As such, digital dexterity is an essential basis for digital literacy.

Digital dexterity depends on basic knowledge of user interface technologies and some experience in using these technologies. Traditional digital technologies that have been used for decades in user interfaces of digital devices are the following:

- Typing devices (like keypads and keyboards)
- Pointing devices (like mice and trackballs)
- Audio devices (like microphones and speakers)
- Video devices (like screens, projectors and cameras)

This set of technologies is expanding, however. With the advent of new technologies, these may become part of required digital dexterity. An example technology class that has become highly popular since about 2005 is the *touch screen* for interactive input. The introduction of the touch screen first brought the basic user actions of *tapping* and *swiping* into the scope of digital dexterity and *multi-touch* actions later. Currently, touch screens are the de-facto interface for mobile digital devices and are becoming increasingly popular in stationary digital devices. Newer example technology classes are virtual reality (VR) [11] and augmented reality (AR) [12], which bring new user interface devices such as VR and AR headsets to various application domains (an interesting example is the cultural heritage domain [13]).

It is noteworthy that the advent of new digital user interface technologies can have specific consequences for social groups with special needs, such as the elderly, the visually impaired and the hearing impaired. On the one hand, these technologies can open up new possibilities of interaction. An example is automatic text-to-voice conversion for the visually impaired. On the other hand, these technologies can introduce new barriers for interaction, such as the complexity of multi-touch interfaces for the elderly.

In electronic business settings, we also see the advent of new technologies. In business-to-business communication contexts, we see for example the fast and widespread emergence of electronic meetings and electronic conferences, which require digital dexterity with advanced audio and video devices. Newer technologies like VR and AR also recently made their way into specific electronic business applications, for example for immersive data analysis, remote assistance and virtual presentation of products. Combinations of technologies have been moving in the direction of *virtual presence* or *telepresence* [14], i.e., providing an experience like physical presence at a remote location through digital means. This is applied, for example, for conducting business meetings [15].

4. Digital Proficiency

The level of digital proficiency of an individual determines to what extent that individual is able to reach specific goals by the use of digital technologies, i.e., in a process in which these digital technologies are essential. The notion of digital proficiency is closely related to the competences described in the DigComp framework [9]. Goals in the context of digital proficiency can be of a personal or of a business nature. Typically, a sufficient level of digital proficiency cannot be reached without an adequate level of digital dexterity, as described in the previous section.

4.1. Digital Proficiency for Personal Goals

Digital proficiency for personal goals covers a broad spectrum of activities. Examples of digital proficiency elements to reach personal goals are the ability to engage actively in social media, the ability to autonomously perform an electronic banking transaction and the ability to autonomously buy a product in a virtual shop on the Web. The latter two examples are in the business-to-consumer domain of electronic business [2], so these

personal goals can be explicitly related to electronic business. The first example typically makes use of platforms of a commercial nature, so this goal is implicitly related to electronic business. This implicit relation is shown, for example, by the fact that the individual is typically exposed to commercial advertising on social media platforms.

Studies have shown that digital proficiency for achieving personal goals can vary between groups of individuals with specific profiles, for example, profiles related to age [16]. This implies that programs to improve digital proficiency need to be designed to take these differences into consideration.

4.2. Digital Proficiency for Business Goals

Digital proficiency for business goals covers a wide array of aspects. Examples of digital proficiency elements to reach business goals are the ability to perform administrative tasks in an automated information system, the ability to compose a document with word processing software and the ability to have a meeting using video conferencing. The latter is part of electronic business in the inter-organizational sense of the term [2], as it supports digital collaboration between organizations.

The COVID-19 pandemic has dramatically reduced face-to-face interaction in business and consequently resulted in a large increase in the use of digital collaboration. This has led to high requirements with respect to adequate levels of digital proficiency, both with respect to reaching business goals, but also with respect to guarding one's health in (almost) purely digital business interaction.

5. Digital Awareness

Digital awareness is interpreted as the level to which an individual is able to understand the consequences of participating in digital interaction. This can be interpreted as the *reflective level* of digital proficiency, related to critical thinking skills [17] when using digital channels in the electronic business domain. This reflective level is related to several of the competences listed in the DigComp framework [9], such as "Competence 1.2: evaluating data, information and digital content", but these competences are formulated on a more operational level in DigComp. Digital awareness can in principle be reached without digital proficiency (as one can understand the consequences of actions without being able to perform these actions) but becomes most essential when an individual actively uses his or her digital proficiency to achieve goals.

An adequate level of digital awareness is essential for participating in electronic business (in the broad interpretation of the term, including digital society at large) in a responsible way, both with respect to the participating individual and with respect to the digital community the individual is participating in. An important element in this context is managing the digital identity [18] of an individual (it is therefore explicitly included in the DigComp framework [8,9]). This is becoming increasingly important in both private and professional contexts, where traditional means of identification (often of a physical nature) are replaced by digital ones (which have a virtual nature). In a broader context, digital awareness is an essential ingredient of digital citizenship [19].

The consequences of participating in digital interaction can be of a positive nature or of a negative nature, all of which need to be understood to be adequately digitally aware. Consequences of a positive nature are often coupled to the goal of a digital interaction and hence desired. For example, actively participating in social media leads to the consequence of the possibility of new friendships. Consequences of a negative nature are usually not desired, but intrinsically linked to the performance of the interaction, often in an implicit way. Below, we focus on important classes of negative consequences. As awareness of these is not always obvious and, consequently, they require explicit attention in the formation of digital awareness.

5.1. Threats to Privacy

A well-known—but often neglected—negative consequence is the threat to privacy. In digital interaction, personal data are often entered into digital systems or acquired by digital systems. It is not always clear what can be done with these data by the owners of these systems. Modern laws (like the European General Data Protection Regulation or GDPR [20]) regulate this to some extent, but these do not avoid the use of data with consent of the owner of these data. To the owner, it is not always clear what he or she is consenting to, as this is often described in long and complex consent descriptions.

The advent of digital identities allows for easy unique identification of individuals across applications of electronic business, thereby opening up new ways for cross-linking data on individuals. This can pose new threats to privacy, as data items that are individually not that privacy-sensitive can be combined to knowledge about an individual that is far more privacy-sensitive. An example is customer profiling in electronic retail or in digital communication.

5.2. Threats to Safety

An often directly dangerous negative consequence of digital interaction is the possibility of becoming a victim of *cyber-crime* [7]. A typical example of cyber-crime is known as *phishing*, in which malicious organizations portray themselves as benevolent organizations to obtain important personal data from victims, such as their banking details. In digital interaction, this threat is usually much greater than in traditional, physical interactions, as the true identity of involved organizations and individuals is harder to establish. Phishing can target both individuals and business organizations and is increasing significantly in volume since the level of digital interaction increased [21].

Another dangerous negative effect of digital interaction is the risk of *cyber-bullying* [22], i.e., using digital channels for abusing individuals. Cyber-bullying can take place in many contexts, but is often observed in adolescent circles, for example in schools.

5.3. Threats to Unbiased Opinion

The widespread use of digital services for performing tasks with either a personal or a business character can lead to a threat to unbiased opinion. This threat has a more explicit and a more implicit component. Both the explicit and implicit components can lead to a threat to the formation of unbiased opinions. An adequate level of digital awareness should enable an individual to effectively handle this threat.

The more explicit component of the threat is formed by the choice of channels used to gather information for performing a task, for example the use of specific search engines. Many well-known and broadly used search engines have commercial goals (as they engage in electronic business), so they may present the information requested by users in a way that is biased by these commercial goals. Sponsored links are a very clear and explicit example of this. A less clear example is the way search results are ordered by the engine and presented to a user, which can heavily influence his or her processing of this information.

The more implicit component is formed by the presentation of information that is not requested by a user but delivered to this user for other reasons that are inspired by the business objectives of the operator of a digital platform. Advertisements in search engine results and on social media pages obviously go into this category, but other unsolicited information as well.

5.4. Threats to Freedom-of-Choice

A negative consequence of digital interaction that often receives too little attention is the threat of the loss of freedom to choose the digital channels for performing specific actions, such as the acquisition of goods or the use of information services. This loss of freedom-of-choice can be created by *vendor lock-in* situations [23] that are created by large, commercial digital platform operators. We discuss this in the context of loss of freedom

of individuals, even though the threat also exists for organizations engaging in digital interaction (creating *business-to-business vendor lock-in*).

In current business-to-consumer e-business, we see the emergence of large digital platforms that offer services to consumers in areas like social engagement, messaging, schedule management, shopping, entertainment and travel planning. The most prominent of these platforms are operated by large players in the electronic business arena, which operate multiple platforms with complementary functionalities or single platforms with multiple integrated functionalities. In both cases, it is both operationally effective and efficient for individual users to use multiple services from the same operator; this creates seamless integration of services within the ecosystem of the operator. When the number of services used from the same operator grows, however, the dependency of the individual on the services of the operator grows as well, leading to a loss of freedom-to-choose. Obviously, an individual can choose not to use the operator anymore, but the costs to change can be large, either from a financial or from an effort perspective, or both. These costs are generally referred to as *switching costs* [23].

Understanding the effect of vendor lock-in as part of digital awareness is essential to guard the freedom to choose digital services (and the information delivered by them) by individuals in the current time frame in which the power of a small set of large service providers is growing.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

Entry Link on the Encyclopedia Platform: https://encyclopedia.pub/15028.

References

1. History of Personal Computers. Available online: https://en.wikipedia.org/wiki/History_of_personal_computers (accessed on 1 June 2021).
2. Grefen, P. *Beyond E-Business: Towards Networked Structures*; Routledge: Abingdon, UK; New York, NY, USA, 2016.
3. Evans, P.; Wurster, T. *Blown to Bits: How the New Economics of Information Transforms Strategy*; Harvard Business Review Press: Boston, MA, USA, 1999.
4. Timmers, P. *Electronic Commerce: Strategies and Models for Business-to-Business Trading*; Wiley: Chichester, UK, 2000.
5. The Rise of the Smartphone: 20 Years of Mobile Innovation. Republic Wireless. 2013. Available online: https://visual.ly/community/Infographics/technology/rise-smartphone-20-years-mobile-innovation (accessed on 6 June 2021).
6. Kelly, G. *The Digital Revolution in Banking*; Occasional Paper 89; Group of Thirty: Washington, DC, USA, 2014.
7. Cyber Crime. National Crime Agency, UK. Available online: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (accessed on 6 June 2021).
8. *A Global Framework of Reference on Digital Literacy Skill for Indicator 4.4.2*; Information Paper No. 51; UNESCO: Paris, France, 2018.
9. DigComp: Digital Competence Framework for Citizens. Available online: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework (accessed on 24 May 2021).
10. Soule, D.; Puram, A.; Westerman, G.; Bonnet, D. Becoming a Digital Organization: The Journey to Digital Dexterity. 2016. Available online: https://ssrn.com/abstract=2697688 (accessed on 25 May 2021).
11. Bailenson, J. *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do*; W. W. Norton & Company: New York, NY, USA, 2019.
12. Cronin, I.; Scoble, R. *The Infinite Retina*; Packt Publishing: Birmingham, UK, 2020.
13. Bekele, M.; Pierdicca, R.; Frontoni, E.; Malinverni, E.; Gain, J. A survey of augmented, virtual, and mixed reality for cultural heritage. *J. Comput. Cult. Herit.* **2018**, *11*. [CrossRef]
14. Rae, I.; Venolia, G.; Tang, J.C.; Molnar, D. A Framework for Understanding and Designing Telepresence. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*; ACM: New York, NY, USA, 2015; pp. 1552–1566.
15. Standaert, W.; Muylle, S.; Basu, A. An empirical study of the effectiveness of telepresence as a business meeting mode. *Inf. Technol. Manag.* **2016**, *17*, 323–339. [CrossRef]
16. Arning, K.; Ziefle, M. Barriers of information access in small screen device applications: The relevance of user characteristics for a transgenerational design. In *Universal Access in Ambient Intelligence Environments*; Lecture Notes in Computer Science; Stephanidis, C., Pieper, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4397. [CrossRef]
17. Ennis, R.H. A concept of critical thinking. *Harv. Educ. Rev.* **1962**, *32*, 81–111.
18. Camp, J.L. Digital identity. *IEEE Technol. Soc. Mag.* **2004**, *23*, 34–41. [CrossRef]

19. Mossberger, K.; Tolbert, C.J.; McNeal, R.S. *Digital Citizenship: The Internet, Society, and Participation*; MIT Press: Boston, MA, USA, 2008.
20. General Data Protection Regulation-GDPR. Available online: https://gdpr-info.eu/ (accessed on 26 May 2021).
21. New Research Shows Significant Increase in Phishing Attacks since the Pandemic Began Straining Corporate It Security Teams. *Secur. Mag.* **2020**. Available online: https://www.securitymagazine.com/articles/93194-new-research-shows-significant-increase-in-phishing-attacks-since-the-pandemic-began-straining-corporate-it-security-teams (accessed on 6 June 2021).
22. Slonje, R.; Smith, P.K. Cyberbullying: Another main type of bullying? *Scand. J. Psychol.* **2008**, *49*, 147–154. [CrossRef] [PubMed]
23. Vendor Lock-In. Wikipedia. Available online: https://en.wikipedia.org/wiki/Vendor_lock-in (accessed on 6 June 2021).