The development of e-services in agricultural social security – opportunities and threats

Robert Żółtaszek

Abstract

For an increasing part of the Polish society, the digital transformation must take place evenly across all social groups in order to be able to support the development of our economy and become its driving force. The development of e-services and e-government constitutes an inevitable process that should be properly moderated by the state, and in some areas even stimulated and driven. Developing digital competences in the social group of farmers is important from the perspective of equality of access to modern services, technologies, and e-state. Proper development of this space may constitute an additional driving force of our economy, and be its supporting engine determining new levels of competitiveness. Since 2015, the Agricultural Social Insurance Fund (KRUS) actively participates in this process by creating and constantly developing the eKRUS platform, which enables online access to an increasing number of services that so far have been provided to farmers only by traditional means in Local Branches. This paper presents current achievements in the field of e-government, as well as the opportunities and risks associated with digitalizing public services. Only conscious individuals, constantly developing their digital competences are able to efficiently and safely navigate through the virtual space that absorbs most of our lives.

The aim of the study is to present on-line public administration services available in Poland, mainly the integrated eKRUS platform, focusing particularly on the degree of its utilization by farmers, and indicating factors inhibiting the development of e-government in the above-mentioned social group, as well as the ways of eliminating them. The paper indicates the need to develop methods of increasing the e-competences of farmers and ways of reaching this professional group with new tools developing the above skills.

Keywords: cybersecurity, e-administration, eKRUS, e-state, trusted profile, farmers.

Robert Żółtaszek, PhD, postgraduate student of "Agricultural social insurance, functioning, administration, and legal aspects" course, head of the KRUS Local Branch in Turek, Agricultural Social Insurance Fund (KRUS).

Introduction

In the last decade, the global development of the digital society has accelerated every year, and the period of the pandemic caused by the SARS-CoV-2 virus provided additional impulses to the following development of e-service, e-labour, and e-learning. Every day we take advantage of an increasing number of services available via a computer network (online[1]). The process of transferring an increasing part of human life to the virtual space located on the Internet[2] could not go unnoticed or ignored by state institutions. Along with the development of commercial services, the development of e-state and e-government slowly took place, and the universal online access to public services became essential for the country's further socio-economic development. Moreover, it has to be stated that such development (e-development) and its scale will constitute an advantage of social and economic competitiveness in the European and global environment. The number of people taking advantage of e-government is steadily increasing year by year. In 2021, 47.5% of the Polish society used public administration services via the Internet. The increasing percentage of people taking advantage of this tool for handling official matters is significant not only socially but also economically. The pandemic and lockdown made us realize the significance of this element of our lives, as these events disrupted the daily life of many Poles, and even interrupted access to such obvious services as schools, offices, doctors, banks, or the post office. Along with the development of the e-world, its dark side also develops, posing a great threat to unaware individuals. Diseases are not only human problem. The digital world is also full of infections, but they concern devices such as computers, phones, tablets, printers, routers, etc. In the virtual world, infections are caused by "germs", namely m a l w a r e[3], i.e., a large family of malicious software, covering such programs as viruses, worms, Trojans, adware, auto-dialers, or other malicious tools. A continuous, wide-scale education of the general public that would address the issue of safe online navigation, as well as the development of broadly understood e-competences are necessary to continue the fast development of e-community, e-government, and e-state. Famers form a social group that is also interested in using e-state services. Since 2015, the eKRUS platform has been actively and continuously developed[4], providing access to the services of the Agricultural Social Insurance Fund.

1. Polish dictionary, https://sjp.pwn.pl/slowniki/ONLINE.html, access 20.04.2022.
2. Wikipedia, https://pl.wikipedia.org/wiki/Internet, access 20.04.2022.
3. Sekurak, https://sekurak.pl/robak-trojan-wirus-o-co-w-tym-wszystkim-chodzi/, access 20.04.2022.
4. The IT system of the Agricultural Social Insurance Fund, https://www.ekrus.gov.pl/p4b-web/index.html, access 20.04.2022.

The aim of the study is to present on-line public administration services available in Poland, mainly the integrated eKRUS platform, particularly stressing its usage by farmers and indicating the factors inhibiting the development of e-government in the above-mentioned social group, as well as ways of eliminating them.

e-Citizen, e-State

One can often hear the terms e-society, e-state, e-government, or e-services. All such terms, with the prefix *e-* indicate the existence of a parallel world – an online world with unlimited resources and possibilities. Distance and opening hours no longer matter. Everything is open 24/7 from any location in Poland and the world, from any device with access to the Internet. The Internet has revolutionized the flow of information and access to commercial services, and thus also revolutionized every state through the access to public offices and information. For example, the Polish State develops and expands the offer of public services available via the new information and communication technologies (ICT). The Central Statistical Office defines the concept of e-government[5] as "Electronic public administration consisting of using ICT, compounded with organisational changes and new skills in public administration in order to improve public services and democratic processes and to strengthen the support of programmes created by the public administration". Currently, the main electronic platform – www.gov.pl – is being developed in one place, grouping and integrating the previous platforms intended for citizens, entrepreneurs, officials, and farmers.

The modern farmer faces an exceptional situation, because with the gov.pl platform they can simultaneously use the e-office not only as a citizen and a farmer, but often also as a person conducting business activity from the position of an entrepreneur.

Examples of categories of issues that can be handled in the e-office for a citizen[6]:

- Documents and personal data – identity card, passport, driving license, access to and changing personal data, contact details;
- Education – remote lessons, nursery, kindergarten, primary school, high school, technical school, industry school, studies;
- Drivers and vehicles – driving license, vehicle registration, registering out a vehicle, penalties and fines, parking;

5. Main Statistical Office, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1769,pojecie.html, access 20.04.2022.
6. Service of the Republic of Poland, https://www.gov.pl/web/gov/uslugi-dla-obywatela, access 20.04.2022.

– Residence and elections – permanent residence, temporary residence, elections, voting;
– Real estate and environment – land and mortgage registers, housing, taxes and environment, surveying and cartography;
– Taxes – tax on: income, inheritance, donations, and civil law transactions;
– Legal assistance – assistance for consumers, help-line, report a crime or offense;
– Labour and business – employment, own business, subsidies, taxes;
– Family and marriage – child, benefits for children, marriage, family, family problems;
– Military and security – military service, veteran, security, help-lines;
– Travel and leisure – insurance, travel abroad, travel of children;
– Benefits and financial assistance – child support, housing assistance, difficult situation, health benefits;
– Certificates and copies – civil status records, National Court Register and National Criminal Register, land and mortgage registers, register of identity cards;
– Health and social insurance – treatment, rehabilitation, disability, pension, retirement, insurance, funeral;
– Foreigner in Poland – obtain a PESEL number.

Examples of categories of issues that can be handled in the e-office for an entrepreneur[7]:

– Anti-crisis shield – support suite for entrepreneurs under the "Anti-Crisis Shield" government program;
– Establishing a business – choose the type of business you want to run and learn how to start one,
– Company development – find out how to develop your company and where to find financing;
– Employees in the company – check what are the rules for hiring employees, their rights and obligations;
– Taxes and accounting – learn how to settle taxes and handle bookkeeping;
– Social insurance – check how to deal with insurance matters in ZUS/KRUS;
– Official matters – learn how to handle business affairs in offices;
– An entrepreneur's obligations – learn your obligations when running a company;
– Permits, concessions, registers – permits, concessions, entries in registers of regulated activities, certificates;

7. Service of the Republic of Poland, https://www.gov.pl/web/gov/uslugi-dla-przedsiebiorcy, access 20.04.2022.

– Professional qualifications – check how to handle matters related to qualifications concerning your profession;
– Changes in the company – check how to make changes in a company and how to report them to offices;
– Suspension and resumption – handle matters related to suspending and resuming activity;
– Closing a company – how to handle matters related to closing a company, sale, inheritance, bankruptcy;
– Sales and marketing – learn the rules of introducing products/services to the market;
– Contractors and customers – check what are the principles of reliable cooperation with contractors and customers;
– Foreign trade – learn how to conduct foreign trade within and outside the EU;
– Doing business in the EU – check how to run your own business within the European Union;
– Construction investments – handle formalities related to implementing construction investments in the company;
– Foreigners in Poland – check the rules of conducting business in Poland by foreigners.

Categories of matters possible to be handled in the e-office for a farmer[8]:

– Financial support, operating subsidies – direct payment, estimating agricultural crop losses, excise duty on agricultural fuel;
– Social insurance – pension, retirement, maternity benefit, funeral benefit, health and social insurance;
– Certificates, permits, and registers – official register of professional entities, permits, seed, supervised activity;
– Plant cultivation – phytosanitary certificate, organic and conventional seed, agricultural crop losses, organic farming, sale of agricultural land;
– Animal husbandry – animal hygiene and housing conditions, supervised activity, Communicable Disease Act, identification and registration of animals;
– Real estate and agricultural land – agricultural land trading, sale, purchase, advertising portal.

In addition to the above categories, e-citizen has an access to separate platforms such as:

– ZUS Electronic Services Platform (ZUS-PUE),
– Electronic inbox (ePUAP),

8. Service of the Republic of Poland, https://www.gov.pl/web/gov/uslugi-dla-rolnika, access 20.04.2022.

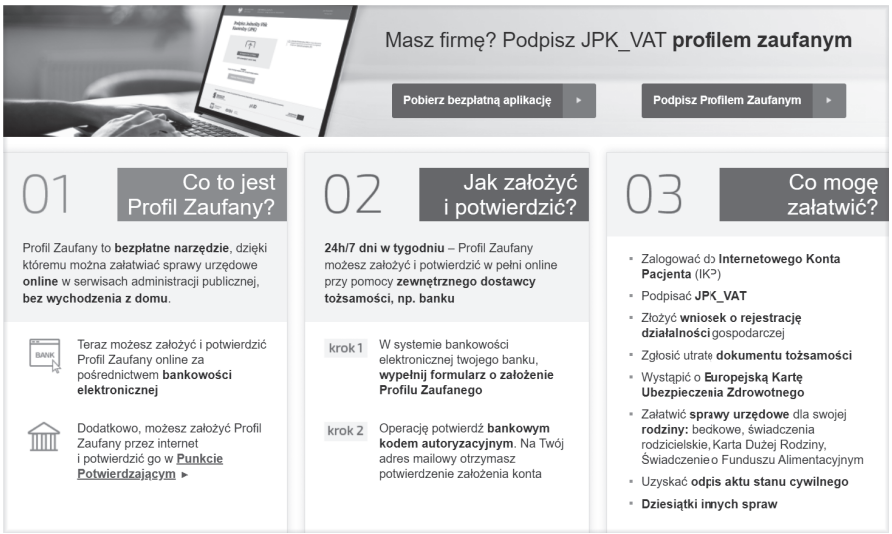
– Internet Patient Account,
– Central Records and Information on Business Activity (CEIDG),
– Central Register of Vehicles and Drivers (CEPiK),
– Electronic Land and Mortgage Register System,
– Tax portal,
– Geoportal etc.
– Usage of the e-world or e-government requires a key, thanks to which the citizen can safely confirm their identity. The key that opens the digital world consists in the Trusted Profile and/or the Qualified Signature, which act as virtual signatures.

The Trusted Profile[9] (PZ) is a free tool made available by the state, that allows performing the following actions:

– confirm your identity in electronic administration systems,
– sign a document with a qualified signature.

The Trusted Profile is used only for contacting public administration (e.g., offices, ministries). It is valid for three years with the possibility of extending it for another three years. It is unique, assigned to only one user, and therefore it should not be shared with anyone.

Figure. 1. Information about the Trusted Profile



Source: Profil Zaufany, https://pz.gov.pl/pz/index, access 20.04.2022.

9. Information and service website for entrepreneurs, https://www.biznes.gov.pl/pl/portal/0074, access 20.04.2022.

More than ten years have passed since the implementation of PZ (2011), and until 2016 it has been mainly used by officials (approx. 400,000 PZ accounts). In 2019, only three million accounts were created. A radical change took place since 2020, and there has been a great increase in the number of created PZ accounts. At the end of 2020, there were already eight million active PZ accounts. In March 2022, their number reached 14 million, and only since the beginning of this year, citizens have created 600,000 new PZ accounts[10].

Qualified Signature[11] (PK) has a wider application than PZ. It is not limited to official matters, as it can be used to conclude distance contracts and participate in tenders. It has the same legal force as a handwritten signature and is a paid service, this is why it is most often used by private companies.

Poland did not stop at the above mentioned identification and authentication tools. On March 4, 2019, a solution was introduced consisting in embedding an electronic layer (chip) into all newly issued identity cards (e-cards). Using an e-card requires a special reader connected to a computer, or a phone equipped with NFC technology (Near Field Communication). Having an appropriate reader supporting e-cards, we can efficiently and conveniently log into e-services of public administration portals without a login or a password. The electronic layer embedded into the ID card allows signing documents and sending them electronically (thanks to a personal signature).

Further development of the information and communication infrastructure allowed creation of a special app for phones – mObywatel[12]. This app went a step further in digitalizing our lives as it allows us to have constant access to e-government via our phones.

mObywatel constitutes a type of digital wallet containing documents and enabling access to e-services. This app allows:

– securely retrieving and presenting your data,
– quickly and effectively logging in to the e-Tax Office and settling your tax report,
– securely using an eRecepta (medical prescription) without providing the PESEL number,
– using discounts, privileges for large families,
– presenting a confirmation of COVID-19 vaccination,
– presenting the driver's license and verifying penalty points,
– showing and verifying car data,
– using school or student mLegitymacja (student card).

10. Data of Chancellery of the Prime Minister of March 10, 2022, Service of the Republic of Poland, https://www.gov.pl/web/cyfryzacja/14-milionow-profili-zaufanych2, access 5.05.2022.
11. Information and service website for entrepreneurs, https://www.b biznes.gov.pl/pl/portal/0075, access 20.04.2022.
12. Service of the Republic of Poland, https://www.gov.pl/web/mobywatel, access 20.04.2022.

Table 1. People using the mObywatel app in 2021

Specification	People using the mObywatel app
Total	**5,484,806**
including	
EU Covid certificate	4,429,933
mPrawo jazdy (driving licence)	3,294,120
mPojazd (vehicle)	2,300,466

Source: Central Statistical Office, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,1,15.hml, access 2.05.2022.

Throughout 2021, the percentage of people aged between 16 and 74 and taking advantage of e-government services amounted to 47.5%, what constitutes an increase of 5.6 percentage points compared to the previous year[13]. In the group of on-line activities, the largest increase was recorded for sending completed forms – an increase by 6.4 percentage points compared to the previous year. For example, browsing information on public administration websites increased by approximately 2 percentage points. The group of people actively contacting various offices in order to deal with their matters also grows with each year.

Table 2. People using public administration services via the Internet

Specification	2020	2021
People using public administration services via the Internet	**41.9%**	**47.5%**
in order to:		
search for information on public administration websites	27.2%	29.4%
download official forms	25.4%	27.4%
send filled-out forms	33.5%	39.9%

Source: Central Statistical Office, Informational brochure "Społeczeństwo informacyjne w Polsce w 2021 roku. Informacja sygnalna", www.stat.gov.pl, access 27.04.2022.

The number of people taking advantage of e-government is steadily increasing every year. A wider inclusion of the society in the process of the state's digitalization is of significant social and economic importance, prevents digital exclusion, increases

13. Main Statistical Office, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,2,11.html, access 27.04.2022.

the availability of e-services of state institutions, and reduces queues in offices. This also involves developing proper e-competences and creating a safe user environment. E-government stands primarily for quick access to information, convenience of interested parties, saving time, as well as an uniform, high quality of service. Both economic aspects and better perception of Poland by foreign investors work in favour of digitization. According to a report by McKinsey & Company of 2018 entitled "Poland as a Digital Challenger – Digitalization as a new growth engine for the country and the region"[14] (PL: *Polska jako Cyfrowy Challenger – Cyfryzacja nowym motorem wzrostu dla kraju i regionu*) thanks to digitalization, Poland's GDP may increase by an additional 64 billion Euros and reach 15% of GDP by the year 2025.

eKRUS – Farmers' Portal

The name eKRUS[15] refers to the IT system of the Agricultural Social Insurance Fund, widely available via the Internet, and its purpose is to provide online support for the people insured at the Fund.

eKRUS was created for:

- farmers and the spouses of farmers,
- household members subject to social insurance for farmers (USR) or health insurance (UZ),
- family members registered for health insurance.

Initially, from July 3, 2015, the eKRUS Farmers' Portal was implemented in the KRUS Regional Branch in Rzeszów and its subordinate local branches, and from 2016 it has been used throughout the Fund.

In order to be able to use the Farmers' Portal, it is necessary to register and create a user profile. This can be done in three ways:

- in the form of a printed application – it has to be filled-out and printed from the website, signed by hand, and then submitted at a KRUS Local Branch or completed directly at a local branch;
- in the form of an electronic application – this is the easiest method consisting in providing your personal e-mail address and signing the form with your Trusted Profile;

14. McKinsey & Company, https://www.mckinsey.com/pl/our-insights/polska-jako-cyfrowy-challenger, access 5.05.2022.
15. The IT system of the Agricultural Social Insurance Fund, https://www.ekrus.gov.pl/p4b-web/index.html, access 10.05.2022.

– in the form of an ePUAP application – log in to the ePUAP platform, then indicate a given office, search for the application, and fill it out. The application is confirmed with the use of a Trusted Profile or other electronic signature, and then it is forwarded electronically for consideration by the Service Provider.

When logging into the eKRUS system for the first time, it is necessary to provide a username (login) and password, and accept them. The user will be required to change the password to a different and secure one, and complete an auxiliary question along with the answer to it. The answer to this question will be needed in the process of regaining access to your account. In the event of exceeding the limit of login attempts, i.e., providing an incorrect login and/or password, the system will block the user's account. Access to the account can be recovered using the account recovery function or using login.gov.pl. Additionally, the account can be recovered by contacting technical support or a KRUS Local Branch.

All the necessary information, starting with the methods of creating a user profile of the eKRUS platform up to the methods of current operation are included in a guide located in the Niezbędnik section under the Przewodnik po eKRUS link (in the form of a PDF document)[16].

The eKRUS Farmers' Portal is constantly being developed, expanded and enriched with new capabilities and functions. After logging into the user profile, we gain access to information, documents, and functions regarding, among others:

– the date of the last visit to the portal and failed logins;
– contribution deadlines and amounts;
– a contribution balance list;
– a debt statement;
– information concerning the possible termination of social insurance – insurance on request;
– personal data;
– generating documents such as: (1) certificate of being subject to USR, (2) certificate of periods of being subject to USR, (3) certificate of periods of being subject to and paying UZ contributions;
– review of insurance periods and the list of insurance contributions (paid/unpaid);
– reviewing a list of cases concerning USR;
– reviewing reminders and notifications;
– cases concerning farmer's assistant;

16. The IT system of the Agricultural Social Insurance Fund, https://www.ekrus.gov.pl/p4b-web/static/eKRUS_Przewodnik_20220428.pdf, access 10.05.2022.

– browsing the message box addressed to the insured;
– payments of contributions and debts due to USR and UZ.

The eKRUS Farmers' Portal is one of the very few public e-services platforms that, on its website, includes thoroughly described Safety Rules[17] that should be followed by every user. The platform above should be given the special mention, because its security policy stresses the significance of verifying the correctness of the website URL (Uniform Resource Locator – a uniform address format) before logging in, and the SSL certificate (Secure Sockets Layer), which is used to authenticate the server. The network security principles will be discussed in more detail in the next section.

At the end of the first quarter of 2022, there were 14 million active PZ users out of 38,028,000 citizens of Poland[18], which constitutes almost 37% of the population. Taking into consideration the 3.82% of users of the eKRUS platform compared to the total number of people insured in KRUS, we are aware of how much still needs to be done in this area, and how much potential there is in the social group of farmers.

Table 3. Persons taking advantage of the eKRUS platform

Year	Total number of insured persons	Number of user profiles on the eKRUS platform	Percentage of eKRUS users in relation to the total number of insured
2019	1,199,285	25,445	2.12%
2020	1,173,236	32,596	2.78%
2021	1,134,603	39,500	3.48%
March 31, 2022	1,127,508	43,084*	3.82%

*Data as of May 24, 2022.

Source: Own study based on: Statistical brochure entitled "KRUS w liczbach 2019–2021", https://www.krus.gov.pl/wydawnictwa/broszury-informacyjne-o-krus/, access 15.05.2022; Social Insurance of Farmers Fund, Basic statistical data concerning insured, https://www.krus.gov.pl/krus/krus-w-liczbach/podstawowe-dane-statystyczne-z-zakresu-ubezpieczonych/, access 15.05.2022; Information obtained from the Office of Information Technology and Telecommunication of the KRUS Central, access 24.05.2022.

17. The IT system of the Agricultural Social Insurance Fund, https://www.ekrus.gov.pl/p4b-web/zasady-Bezpieczenstwa.html, access 10.05.2022.
18. Main Statistical Office, https://stat.gov.pl/podstawowe-dane/, access 27.05.2022.

Online safety

The security of the Internet depends on humans. We often hear that people constitute the weakest link in the complex structure of cybersecurity. The above statement can be challenged, however, because even if human is the weakest link, at the same time it can become its strongest element. In order for this to happen it is necessary to constantly develop digital competences, understand the basics of network security, and stay up to date with new threats. This is not difficult with today's free access to information. Usually, the problem with understanding the principles of cybersecurity is related to the lack of basics in this field. To address this problem, basic information concerning e-safety is presented below.

Malware can be divided into various groups depending on type, category, mechanism of operation, or method of infection.

Types of malware[19]

1. Worms – programs that quickly reproduce and spread over the internet, and take advantage of errors, gaps, and vulnerabilities (so-called exploits) in operating systems, especially ones that have not been updated.
2. Trojans (so-called Trojan horses) – software that pretends to be useful or interesting programs, apps that deceive the user. After launching, such an initially harmless file reveals its malicious nature by stealing data, downloading other malicious programs, or giving the remote access to a computer to a criminal. An example is a banking Trojan that allows to steal users' money via electronic banking.
3. Viruses – they add their malicious code to other executable files of the operating system, they have the ability to duplicate and spread to other systems.
4. Bugs – errors, software faults that can distort the functioning of programs, can constitute vulnerabilities and may be used to damage or take over the operating system.
5. Ransomware – this software encrypts all files on the hard drive to request a ransom, the encryption prevents access to computer systems.
6. Spyware – this is a spying software that monitors activity on your computer, such as a keylogger that records typing.

19. KapitanHack.pl, https://kapitanhack.pl/2019/01/08/malware/rodzaje-malware-i-sposoby-na-ich-wykrycie-oraz-ochrone/, access 29.05.2022.

7. Spambots – automated programs designed to send unwanted e-mails (spam).
8. Adware – advertising software that displays unwanted ad content. Such ads may be used by criminals, using the content to lure users. Clicking on them may redirect to unsafe sites or install unsafe programs.
9. Auto-dialers – these are programs used to automatically make phone calls.

Nowadays, a large number of crimes related to new technologies base on social engineering tricks, consisting in influencing people, and using persuasion to commit fraud. Current knowledge concerning new forms of crime is like an invisible shield protecting the society against such threats.

The most common methods of cyber attacks[20, 21]

1. Phishing – one of the most popular attack methods. It consists, among others, in obtaining login data, e.g., to the bank, e-mail box, social media, all kinds of services, as well as to download malware. It is usually conducted via e-mail, text message, website and/or an online messenger, and its aim is to make a person click on a link, download and open the attachment, log in to a website imitating a real website, or provide personal data, credit card details, etc.
2. Spear-phishing – this is a phishing attack aimed at a specific person.
3. Smishing – a type of phishing, a message sent from an Internet gateway pretending to be sent by a service provider, e.g., a bank or a power company. The website through which the text messages are sent allows providing any phone number. This causes such messages to be received in the same place as text messages, e.g., from a bank. Such a message most often encourages a person to click a specified link.
4. Spoofing[22] – consists in pretending to call from a different phone number, e.g., from a bank or office and making a call to the attacked person. The number displayed on the phone of the targeted person is an actual number of e.g. bank, luring the mark into disclosing sensitive data. This is the most common way personal data, blik data, credit card number, or online account login data are acquired, although spoofing is also commonly used for managing property in an unfavourable manner. Online messengers are used for this purpose.

20. CERT Polska, https://cert.pl/posts/2022/05/krajobraz-bezpieczenstwa-polskiego-internetu-w-2021-roku/, access 9.05.2022.
21. CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2020.pdf, access 9.05.2022.
22. Niebezpiecznik.pl, https://niebezpiecznik.pl/post/cyberalerty-darmowa-aplikacja-od-niebezpiecznika-ostrzegajaca-o-atakach/, access 30.05.2022.

5. Vishing[23] – or voice phishing, this method does not require criminals to possess information technology knowledge. The aim is to obtain confidential information and/or persuade the victim to perform a specific task, e.g., install an app on a phone or computer, or to transfer valuable possessions to a person impersonating a police officer.
6. Whaling – an impostor claims to be someone important, e.g., a director. Most often, the impostor persuades the victim to perform a specific task, e.g., make a money transfer, disclose personal or company data.
7. Pharming[24] – is a type of phishing including advanced information technology without the social engineering element. It is very dangerous due to the method of the attack. The only protection against it is good antivirus software. This method involves redirecting to fake websites pretending to be other legitimate and trusted websites. An overlay for a banking app is created in terms of phones. That is how login data to, for example, online banking is stolen.

The above list does not cover all fraud methods, but indicates their main directions and modes. The victim is always persuaded to act, whether out of fear and curiosity or greed. The impostor intentionally exerts pressure to reduce the time to think and persuade the victim to perform specific actions.

Threats

Phishing campaigns are regularly carried out in the world and in Poland, and so are various sorts of fraud using social engineering tricks and/or related to the installation of unwanted malware that steals confidential data, gives remote access to the device[25].

Examples of campaigns:

1. SMS, e-mails from criminals imitating banks, service providers (e.g., PGE, Energa, DHL, inPost), or online stores that encourage clicking on a false link, downloading and installing malware. In this way, criminals take over the phone or computer and steal the data on the devices that allows them to log in to various websites, banks, or e-mail. Links also redirect to fake payment gateways stealing credit card or debit card details.
2. SMS messages from mObywatel (imitating the real app) informing about a following vaccination dose or winning the national lottery, prompting to install malware. The SMS fraud with information about COVID-19 was similar.

23. National Cyber Security Institute, https://kicb.pl/spoofing-i-vishing-poznaj-ich-tajniki-i-nie-daj-sie-oszustom/, access 29.05.2022.
24. Avast Software, https://www.avast.com/pl-pl/c-pharming, access 29.05.2022.
25. CERT Polska, https://cert.pl/zagrozenia/, access 29.05.2022.

3. Advertisements on social networks informing about the possibility of obtaining money after taking action on an indicated website, e.g., entering the customer number to receive additional funds or recommending a bank account to a friend to collect a bonus. This attack makes the target enter their account or credit card details, expiration date, and CVC code.
4. Advertisements on social networks encouraging investing, for example in Orlen or cryptocurrencies. This form of fraud forces you to set up fictitious accounts, provide personal and financial information, or install malware.
5. Search engine ads – cybercriminals take advantage of advertising mechanisms and try to swap the search result to direct the victim of an attack to a fake website.
6. E-mails with attachments to be downloaded, such as invoices, online store policies, regulation or GDPR updates, etc. In this case, there is a risk of downloading malware, enabling macro in Excel files allowing to install malware.
7. Fraud on advertising portals is usually related to communicating with the seller outside the official contact channel and persuading the victim to collect funds for merchandise. In this situation the attacker is redirected to a false bank website and provides personal data to the bank account.
8. Using content to encourage visiting fake websites, most often appearing on social networks, e.g., rape of a minor, the police is asking for help, missile attack on Poland, a footballer earning a fortune. All this information intends to arouse curiosity and cause an outrage. By clicking on it, we are redirected to pages with a false login panel. That is how we may lose our social account, which will then be used to impersonate us, allowing the criminal to e.g., trick our friends to give them money. The "help with voting" fraud on social networks works in a similar manner.

Good practices

The following rules have been developed on the basis of materials included on the CERT Polska website (https://cert.pl/) and safety principles placed on the eKRUS platform (https://www.ekrus.gov.pl). They apply to computers, phones, routers as well as other electronic devices.

1. Update operating systems and web browsers on your devices, create individual user accounts with fewer privileges than the administrator, and enable the firewall.
2. Use antivirus software with an extended toolkit, such as Internet Security. Such software protects additionally against other threats.
3. Update the router firmware, enable the firewall, and change the default administrator password, create a WiFi access password, and it is recommended to enable a guest network.

4. Install software only from legal and trusted publishers, avoid installing software of unknown origin.
5. Protect your app passwords and logins against unauthorized access, and never share them with anyone under any circumstances.
6. Use long passwords with at least 14 different characters (numbers, upper and lower case, special characters), avoid passwords including your personal data, as they may be publicly known.
7. Do not use the same password more than once and for multiple services, as in case of obtaining your password every account can be taken over, change passwords periodically.
8. When using multiple logins and passwords, it is recommended to use a password manager.
9. Wherever possible, enable two-factor authentication, such as email and social accounts, to prevent taking over your accounts. Only a U2F hardware token[26] (e.g., YubiKey) is resistant to phishing attacks.
10. When logging in to a website, always verify the correctness of the URL. Remember that a padlock icon before the address only proves that the connection between your device and the application servers is encrypted with SSL (https, where "s" stands for "secure"), so always check the SSL certificate of the website additionally.
11. Enable additional security tools in browsers, disable automatic password saving.
12. Remember to log out of services and close the browser window, do not leave the device on which you are logged into e-services unattended.
13. When sending important documents electronically, encrypt them before sending, for example with 7-zip software, and send the password to the document by other means.
14. Ignore all requests for logins, passwords or personal data that were sent electronically and over the phone.
15. Always verify the sender of messages forcing you to act immediately through a different communication channel.
16. Suspicious messages in the mailbox can be sent to CERT Polska (https://incydent.cert.pl), SMS messages containing unknown links can be sent to 799 448 084.
17. Optionally, install the free CyberAlert app from Niebezpecznik available in the Google Play Store and Apple AppStore and receive alerts concerning new threats[27].

26. Sekurak, https://sekurak.pl/poradnik-o-kluczach-sprzetowych-na-przykladzie-yubikey-5-nfc-2fa-u2f-fido2/, access 30.05.2022.
27. Niebezpiecznik.pl, https://niebezpiecznik.pl/post/cyberalerty-darmowa-aplikacja-od-niebezpiecznika-ostrzegajaca-o-atakach/, access 23.08.2022.

Conclusion

The main objective of the study was to present the opportunities and threats related to the development of e-services in the social group of farmers. The development of e-government in Poland has accelerated in recent years, and new solutions were introduced. The scope of issues that can be handled on-line has been extended. Many citizens, especially during the pandemic, noticed the positive aspects in their contacts with the e-government. A convenient, queueless service system gains an ever-increasing number of users. In 2020, the percentage of people taking advantage of public administration services via the Internet amounted to 41.9%, and increased in the following year by 5.6 p.p. reaching the level of 47.5%. Currently, more than 5.5 million Poles use the mObywatel app. The most impressive increase concerned the number of Trusted Profiles created at the end of the first quarter of this year, i.e., 14 million active PZ accounts. It should also be remembered that the Agricultural Social Insurance Fund contributes to the development of e-government in Poland. The eKRUS platform is constantly being expanded with new functionalities, the number of documents that can be obtained is increasing, and it is also possible to perform payments. The platform is transparent and intuitive. In April 2022, a solution was introduced to eliminate errors occurring during the creation of accounts in the eKRUS Farmers' Portal, namely an additional field with a repeated e-mail address and its confirmation. This small change eliminated errors in the e-mail addresses provided by farmers.

Approximately 37% of Poles have a Trusted Profile, which is a sort of key to our country's e-services. Every year, the number of new PZs is growing, and this process accelerated especially during the pandemic. However, the number of accounts created in the eKRUS Farmers' Portal does not grow so rapidly. The 3.82% of eKRUS users compared to the total number of insured in KRUS looks like a statistical error. This shows how much work there is still to be done in this sphere, and I dare to say that this may require generational changes. However, not waiting for a generational exchange, we can start a process among farmers that will allow us to achieve our objectives.

"Everything is difficult before it becomes easy"

We are afraid of the things we don't understand, and knowledge acts as shield against such threats. Only the development of digital competences in the social group of farmers will provide them with such a protection. Education in the field of digital competences should go beyond the institution of KRUS and involve local

governments and other state institutions. When talking to farmers, it is often possible to hear, quote: "it is difficult"; "I do not understand it"; "I am afraid"; "one more thing that needs to be done on your own". Whenever this is said, the question arises – what can be done about it? Thankfully, there are a lot of ways to address these issues. For example, we can develop patterns of acquiring digital competences on the basis of existing ones, and directing farmers in the right direction to start the process.

It should be emphasized that, in order to succeed in the digital transformation, the trust of citizens in new technologies, their understanding and safe use are essential. This paper not only explains e-solutions of the e-state, but also presents the threats associated with the electronization of everyday life as well as the methods and manners of counteracting such threats.

In order to increase the security of eKRUS users, I propose introducing two-factor authentication when logging into the system. There are various solutions – SMS, authentication apps, or U2F hardware tokens. The first two methods do not protect the user against false websites, which only resemble the real one. For most non-technical people, it is difficult to identify a real domain and distinguish it from a false one. In such a situation, cryptographic keys, e.g., U2F hardware tokens, come in handy. If farmers were equipped with properly configured U2F hardware tokens, logging into the eKRUS platform could be password-free, secure, and fast. Currently, in the USA, it is recommended to phase the SMS account authorization out in favour of safer forms. The Bank of America was one of the first in the world to introduce U2F hardware tokens for logging into its website. Therefore, only a combination of all components: education, security, and convenience can bring measurable effects in the form of increasing the number of eKRUS users. Preparing farmers and equipping them with proper digital competences will not only have a positive impact on the Fund itself, but is also going to accelerate the digitalization of agriculture and become another economic driver. The Fund may be a pioneer in developing safe and easy access to its services, introducing a modern solution such as U2F and providing proper training for farmers, in cooperation with other institutions.

Usage of the integrated eKRUS platform translates to the convenience and quick access to services provided to farmers by KRUS at any time of the day, as well as to saving time and money.

Bibliography

Avast Software, https://www.avast.com/pl-pl/c-pharming, access 29.05.2022.

Główny Urząd Statystyczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1769,pojecie.html, access 20.04.2022.

Główny Urząd Statystyczny, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,2,11.html, access 27.04.2022.

Główny Urząd Statystyczny, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,1,15.html, access 2.05.2022.

Główny Urząd Statystyczny, https://stat.gov.pl/podstawowe-dane/, access 27.05.2022.

Kasa Rolniczego Ubezpieczenia Społecznego, https://www.krus.gov.pl/wydawnictwa/broszury-informacyjne-o-krus/, access 15.05.2022.

Kasa Rolniczego Ubezpieczenia Społecznego, https://www.krus.gov.pl/krus/krus-w-liczbach/podstawowe-dane-statystyczne-z-zakresu-ubezpieczonych/, access 15.05.2022.

Krajowy Instytut Cyberbezpieczeństwa, https://kicb.pl/spoofing-i-vishing-poznaj-ich-tajniki-i-nie-daj-sie-oszustom/, access 29.05.2022.

McKinsey & Company, https://www.mckinsey.com/pl/our-insights/polska-jako-cyfrowy-challenger, access 5.05.2022.

Niebezpiecznik.pl, https://niebezpiecznik.pl/post/spoofing-rozmow-telefonicznych/, access 29.05.2022.

Niebezpiecznik.pl, https://niebezpiecznik.pl/post/cyberalerty-darmowa-aplikacja-od-niebezpiecznika-ostrzegajaca-o-atakach/, access 23.08.2022.

Portal KapitanHack.pl, https://kapitanhack.pl/2019/01/08/malware/rodzaje-malware-i-sposoby-na-ich-wykrycie-oraz-ochrone/, access 29.05.2022.

Profil Zaufany, https://pz.gov.pl/pz/index, access 20.04.2022.

Serwis informacyjno-usługowy dla przedsiębiorcy, https://www.biznes.gov.pl/pl/portal/0074, access 20.04.2022.

Serwis informacyjno-usługowy dla przedsiębiorcy, https://www.biznes.gov.pl/pl/portal/0075, access 20.04.2022.

Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/gov/uslugi-dla-obywatela, access 20.04.2022.

Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/gov/uslugi-dla-przedsiebiorcy, access 20.04.2022.

Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/gov/uslugi-dla-rolnika, access 20.04.2022.

Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/cyfryzacja/14-milionow-profili-zaufanych2, access 5.05.2022.

Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/mobywatel, access 20.04.2022.

Serwis Sekurak, https://sekurak.pl/robak-trojan-wirus-o-co-w-tym-wszystkim-chodzi/, access 20.04.2022.

Serwis Sekurak, https://sekurak.pl/poradnik-o-kluczach-sprzetowych-na-przykladzie-yubikey-5-nfc-2fa-u2f-fido2/, access 30.05.2022.

Słownik Języka Polskiego, https://sjp.pwn.pl/slowniki/ONLINE.html, access 20.04.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, https://www.ekrus.gov.pl/p4b-web/index.html, access 20.04.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, https://www.ekrus.gov.pl/p4b-web/index.html, access 10.05.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, https://www.ekrus.gov.pl/p4b-web/static/eKRUS_Przewodnik_20220428.pdf, access 10.05.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, https://www.ekrus.gov.pl/p4b-web/zasadyBezpieczenstwa.html, access 10.05.2022.

Wikipedia, https://pl.wikipedia.org/wiki/Internet, access 20.04.2022.

Zespół CERT Polska, https://cert.pl/posts/2022/05/krajobraz-bezpieczenstwa-polskiego-internetu-w-2021-roku/, access 9.05.2022.

Zespół CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2020.pdf, access 9.05.2022.

Zespół CERT Polska, https://cert.pl/zagrozenia/, access 29.05.2022.

received: 26.07.2022
accepted: 17.10.2022

This article is licensed under a Creative Commons Attribution 4.0 International license (CC BY 4.0)