Information Horizons: AMERICAN Journal of Library and Information Science Innovation
Volume 01, Issue 02, 2023 ISSN (E): XXX-XXX

Information Security: Modern Realities

Abdullaev Sharof Abdugafforovich
Termez State University, Teacher of the Department of Information Technology

Abstract: *The article discusses the concept of information security, its general meaning, ways to strengthen it, considers ways to protect personal data, considers the concept of information security. Some advice is given to ordinary users.*

Keywords: *information security, information technology, information protection.*

Information technologies are used everywhere, and many can no longer imagine their lives without them: social networks, instant messengers, online stores, online banking - we use all these means of communication and communications, and all these access points are potentially vulnerable. That is why information security plays an extremely important role in our lives. As technology advances, protecting personal data becomes more and more difficult. In this article, we would like to consider the possibilities of solving this problem.

Consider the issues of information security when working with mobile banking applications. Today, customers communicate with banks through the following applications:

- bank-client or online banking through personal computers;
- mobile online applications;
- social networks and instant messengers. Communication channels, according to B. King, are as follows:

At the same time, the client conducts transactions, reports personal data, and is actually vulnerable.

For more than 10 years, jokes have been circulating on the net about artificial intelligence, which, on behalf of the bank, gives advice to clients. The “smart data” marketing trend, which is popular today, involves the maximum personalized collection of customer data, where, based on one common indicator field (mobile phone or email address), you can get a comprehensive portrait of the client.

It would seem, where does information security? By signing a "consent to the distribution of advertising information", automatically pressing the "agree" button, registering in a large number of Internet resources with the same login - all this leads to verification of you as a client, allows you to collect and use personal information.

We note such cases as the analysis of profiles in social networks when applying for a job, contextual advertising, and many others.

Not surprisingly, the protection of personal data in particular and information security in general are of concern to customers.

Usually, information security means the quality of object security, which is most often information, data, system resources, etc.

Information security is the state of data protection, in which their availability, confidentiality and integrity are ensured. In this case, the availability of data means their property, which determines the

possibility of their receipt and further use at the request of authorized persons, confidentiality - the property associated with the fact that these data will not become available to third parties without the consent of authorized persons, and integrity - immutability information during storage or transmission. In other words, to protect information, information must be:

1. sufficiently protected from outside hacking;

2. Operated by a sufficiently educated person;

3. not available to unauthorized persons.

Information security is a set of measures aimed at ensuring information security.

Many organizations build their own information security systems, conduct audits and analyze data security. This applies to both personal data of customers and staff, and information about current activities, financial condition. As a rule, the implementation of protection measures includes organizational measures, for example, the appointment of persons responsible for information security, the development of rules and instructions for users, the implementation of a backup policy, and more. Modern organizations use the requirements of international standards to build information security management systems and use the best world practices [2].

Regardless of the form in which the information is stored, how it is used, it is necessary to implement adequate protection measures. Each manager must objectively assess the current state of information systems, see and understand the needs for information support and existing information problems.

It is for this purpose that the organization should train responsible persons and users in certain aspects of working with data, including the basics of information security. Security software, software, regular updates of anti-virus programs, data encryption are installed.

To improve the organization's data protection, the existing local network is being modernized or repaired, additional video camera equipment is installed, additional servers, uninterruptible power supplies, etc. Due to protection measures, the risks of business information leakage, the risks of various kinds of impacts that cause failures in the operation of information systems, such as like rogue programs, hacker attacks.

No less relevant is the construction of personal information security of users. The use of computers, tablets, smartphones has become an integral part of the life of every student. The modern generation masters information technologies with ease and often pays insufficient attention to the risks that arise when working on the Internet, using removable media, etc. Sometimes only the loss of information or sudden problems with the computer force us to pay attention to strengthening the means of protection and studying the problem of information security.

In everyday life, information protection is mainly considered as protection against virus programs, or viruses. A computer virus is a type of malicious software. It can create copies of itself, embed itself in the code of other programs, boot sectors or system memory areas, and distribute copies of itself through various communication channels. A computer virus was named so for a reason - you can compare its spread with a biological virus. It has many types: Worms, Trojans, Polymorphic viruses and many others. Each of these viruses operates differently, and more and more new viruses are constantly appearing. However, there are countermeasures as well. They are called antiviruses.

Antivirus is a specialized program designed to detect, eliminate and prevent the appearance of computer viruses. Also, one of the functions of the antivirus is the recovery of virus-infected files.

Anyone can protect important information. To do this, it is enough not to ignore some threats. For example, do not use simple passwords. Passwords "0000" on your phone or "parol1" on the mail may well lead to the loss of important data for you. For your password to be strong, it should ideally consist of letters and numbers, have more than 8 characters, contain both uppercase and lowercase letters, and also not match any dictionary word. Virus protection must be used. There are many antiviruses on the market, it is quite easy to choose a simple and effective one. However, before installation, it is better to consult with a specialist. In addition, the installed antivirus should be updated periodically.

You need to learn how to use your computer better. For your computer, the most dangerous hacker is yourself. And if someone else is going to work with your data, you must be sure of his/her competence and integrity. Otherwise, your data may be lost or misused. The software, including the web browser, should be updated periodically. It is very dangerous to go to suspicious pages on the Internet, as well as to pop-up ads. There may be viruses. Users need to use only reliable storage devices. If the device is someone else's and you know nothing about it, there is a risk of connecting a device with a virus to your computer.

In order to secure the use of a computer, you must also remember some aspects of working on the Internet. Under no circumstances should you give out your name, phone number, credit card number, residential address, password, etc. on the Internet. if there is no 100% confidence in the reliability of the source. You need to block spam and ads. Advertising can also be the source of the virus in some cases.

If something in the operation of the computer seems unnatural or disturbing to you, it is better to contact specialists.

Using various methods of protection to the maximum, users create their own information security system that allows them to save their data and minimize the risks of unauthorized access to various kinds of information that is important in life.

Now let's turn to information security issues when using mobile banking applications. Potential client vulnerabilities - password cracking, unauthorized use of bank card and account information, access to information about expenses and income, obtaining information about passwords.

Here are some tips for clients:

- do not use passwords for the Internet and online banking that are already used in other services.
- carefully check where and to whom you pay.
- do not send your bank card details, logins and passwords to online services on unverified sites.
- do not store funds on the card with which you pay via the Internet.
- do not use payments on third party sites.
- Check (or call back the bank) when receiving SMS messages asking for financial information.
- when registering on mass sites, for example, on Avito, use a non-primary email address and phone number.

BIBLIOGRAPHY

1. Кинг Б. Банк 3.0. / Бретт Кинг. – М. ЗАО «ОлимпБизнесс», 2014. – 474 с.
2. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности – Системы управления информационной безопасностью. Требования. – 2005. – 36 с.
3. ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management [Электронный ресурс] // Интернет-портал – URL: http://www.iso.org/iso/catalogue_detail?csnumber=56742 (Дата обращения: 18.09.2017)
4. Базовая информация о информационной безопасности [Электронный ресурс] // Интернет-портал – URL: http://bezopasnik.org/article/1.htm (Дата обращения: 18.09.2017)
5. Федеральный закон «О персональных данных». 27 июля 2006 года № 152-ФЗ. Принят Государственной Думой 8 июля 2006 года