Analysis and Practice of Security Protection Strategy for Mobile Learning

Zhao Wei

Information Center, Xianyang Normal University, Shaanxi Xianyang, 712000

Keywords: Mobile Learning; Security Protection; Measures

Abstract: Mobile learning is actually a way for learners to study at any time and place through mobile devices and mobile Internet, which can make up for the lack of teachers' teaching and social learning. The carrier of mobile learning is a mobile device, which should facilitate access to educational information, resources and services, and can quickly present learning content, providing two-way interaction between teachers and learners. Mobile learning has its own unique advantages, that is, learning anytime, anywhere, using fragmented time learning, low hardware requirements, convenient and timely interaction, etc. In order to ensure the smooth progress of mobile learning, it is necessary to take scientific and effective security measures. Therefore, this paper mainly analyzes the mobile learning security protection measures in detail, in order to provide a powerful help for learners to carry out mobile learning successfully.

1. Mobile learning mode

1.1 Informal learning

In general, informal learning is the opposite of formal learning, and is the way in which learners use informal time and place in work and life to gain knowledge. In informal learning, learners have the right to control the content, time, place, and manner of learning, and close to the real environment, learners often show very strong motivation to learn.

1.2 Situational learning

Situational cognition and learning theory clearly point out that the external learning environment plays an important role in learning. It encourages students not to be limited to the classroom, and to explore in the society. In this process, there are many obstacles to acquiring knowledge. With the strong support of mobile communication technology, learners can acquire knowledge information in an unlimited time and place. And based on mobile communication devices, it helps in the discussion and communication of learning, thus promoting the significant improvement of mobile learning efficiency and quality.

1.3 Contextual learning

Learners have a complete internal world with memories, motivations and experiences. When learners are dealing with new types of knowledge and information, they are related to the internal world, which is the so-called contextual learning. This theory clearly shows the importance of the learner's internal world in learning, and focuses on the detailed analysis of learners' existing knowledge systems, learning motivations and hobbies.

1.4 Activity learning

Activity learning is learning through practical activities, and the ideas come from activity theory. The theory of activity emphasizes interaction and dependence between independent learning and activities. The learning has purpose, enthusiasm, and conscious practicality, including interaction intentions and action reflections, etc. [1].

2. Security protection measures of mobile learning

2.1 Building a three-dimensional server security protection mechanism

2.1.1 Deep protection mechanism of security

The so-called deep protection mechanism is mainly divided into three major elements: organization, technology and management. Among them, network security management achieves effective coordination of the relationship between the three through effective measures and systems, and determines the specific responsibility of technical implementation and security operators so that they can quickly and timely discover security risks. And through the use of scientific and effective measures for risk control, it effectively improves the efficiency of security risk processing, and strengthens the network's comprehensive security capabilities. Therefore, the network security management mechanism needs to solve the human problem first, build a sound security organization system, and effectively solve the close relationship between people and technology, and establish multi-level network security measures, namely, programmatic strategies, security systems, and specific operation process and so on. On this basis, it solves the close relationship between people and operations, adopts safety mechanism measures to ensure network security, and develops safety awareness training for operators, and improves the comprehensive ability of operators by diversified assessment methods. In the daily security protection, we should also pay attention to the interaction between system administrators and security protection technicians, give full play to the role of social platforms, organize WeChat groups, periodically or irregularly publish some developments and hot events about security protection for discussion, providing a powerful help for technicians to continuously update their safety knowledge system. Based on the internal working system, it can also regularly discuss and share internal security knowledge, attaches great importance to the personal safety of technicians, and improves the overall level of security protection.

2.1.2 Introduce reasonable hardware and protection technology of operation and maintenance

Traditional online education and mobile learning programs can be built through the computer room built in the college, but the framework is simple and the basic security facilities are not perfect. To this end, in order to improve the security of mobile learning, commercial cloud services with good stability and reliability can be selected, which are mainly constructed through computer rooms according to international certification standards, and the hardware facilities are relatively perfect.

In terms of cloud service usage, it is necessary to separately divide the application into an internal LAN to effectively prevent other network access phenomena. The operation and maintenance personnel are connected to the bastion machine through the VPN, and enter the internal network with the bastion machine as the carrier. The VPN authentication method is a dynamic password. The dynamic password is implemented based on TOTP, and some of the ports can be simply opened by accessing the machine from the external network, but different systems need to be arranged to the corresponding role users.

2.1.3 Scientific design of the protection mode of the server terminal

Based on software security standards, the platform is fully constructed, and the HTTPS protocol is used to implement network communication, as well as a secure operation and maintenance framework. Among them, the main security layer is built on the outermost layer of the system. In terms of security issues such as injection and authority, it should be effectively solved through integrated measures, and the security layer can also perform independent update and upgrade. Through the JAVA-based SPI mechanism, the imitation process is constructed, and the low-coupling method is adopted to ensure that the general security layer can be consistent with the project [2-3].

2.2 Build a complete Internet communication security protection system

In order to build a sound security system, mobile Internet should strictly abide by established rules. First, in the mobile communication system, security measures that are existing and need to be further strengthened should be actively adopted and scientifically applied through the Internet. That is, assessing network security risks in real time to ensure network stability and reliability. Second, the current mobile communication system is fully analyzed with hidden security threats, and targeted measures are taken to optimize, that is, for network attacks or illegal services, to set and analyze traffic in key aspects of the mobile Internet, and to monitor the installation process of facilities and equipment, so that it can be able to quickly respond correctly and take effective attack protection measures. Third, in conjunction with universities and research institutes, the mobile Internet's related business and environmental characteristics are utilized to develop and design information security technology services to ensure that they have mobile network security features. Mobile network security is mainly involved in links, networks, users, and so on. The mobile network access security policy indicates that the supply caused by the wireless access link is prevented in all directions, and the specific strategy is to realize the security transmission of the data information between the nodes. User security is based on the user security features, the security of data transmission and exchange between the user and the service terminal, and the security features of identity authentication between the two. For mobile learners, they should maintain good mobile Internet usage behaviors, that is, do not use anonymous WIFI, pay attention to the dynamic changes of mobile phone data usage in real time, and change personal hotspot passwords regularly or irregularly.

2.3 Establish a sound mobile client security protection system

2.3.1 Improve learners' information security

Information security literacy is security awareness, knowledge, ability, and information ethics. When the mobile learning project is started, it is necessary to push the common risk warning information in mobile learning to the learner, as well as effective countermeasures, and make suggestions for the learners to cultivate good using behaviors. In addition, mobile learners also need to have a high level of information security. The first is password security, we should absorb the basic knowledge about cryptography, and understand how to set up, using the mobile terminal privacy control function as the carrier, based on website and software guidance, enhance the security level of passwords, and build a security password setting mechanism which meets its own needs. Secondly, we can automatically update the mobile terminal device software and security protection software through application security, and upgrade the APP version independently. Thirdly, we can carry out application security automatic synchronization based on cloud storage and data, and cultivate a good sense of information security and protection. We will carry out personal related information transmission under the established constraints, and we also need to attach great importance to our own hidden data information in the transmission process. Finally, we should absorb the basic knowledge of learning and information security and conduct information security training to ensure information security.

2.3.2 Improve the security technology level of mobile clients

The mobile learning system adopted by universities and educational institutions is mainly developed and maintained by professional software companies, which guarantees the security protection efficiency of mobile clients in terms of hardware and software. First, in terms of hardware, we will intensify efforts to promote security devices through face and fingerprint recognition, and strengthen the physical security level of mobile devices, based on mobile device cameras, combined with mobile learning applications and face recognition. Second, in terms of application software, critical business and personal information modules must provide clear information and risk alerts. Thirdly, in terms of software version update, the existing software version is used as the carrier, adding fingerprint verification, source code confusion, software security reinforcement and other related performances. At the same time, the verification function is added, the mobile version feature value is used as the main basis, the md5 value is set reasonably, and the fixed code assigned to the version is combined to perform encryption, thereby obtaining the final value, and then configuring it on a server-side basis, recording the version in full detail, and clearly indicating whether it can run and whether it is the latest version, and then transferring it to the server for verification. In the case of an unavailable version, a mandatory upgrade is made and the version is converted to an available version. If the available version is not up to date, you are prompted to optimize the upgrade. On the system patch upgrade, the vulnerability patch prompt information is released, and the user is prompted to download and repair. The basic security audit software is added to the system to effectively detect security risks and alert the user to quickly take measures to solve the problem. Fourth, the personal information cancellation function is added through the terminal system to avoid information leakage due to the loss of the mobile device [4-5].

3. Conclusions

All in all, under the rapid development of mobile Internet, smart devices have been widely popularized and widely used, and mobile devices are favored by their own unique advantages, and mobile learning scenarios are becoming more diversified and high-frequency. Therefore, we should build a sound mobile learning mechanism, introduce an application software security framework, establish key indicators for mobile security learning assessment, comprehensively prevent mobile Internet security risks, effectively improve the mobile learning security environment, and provide better mobile learning services for learners.

Acknowledgements

Shaanxi Higher Education Scientific Research Project (No. XGH17160); Special Research Project of Shaanxi Education Department (No. 18JK0834)

References

[1] Li Haojun, Xu Jiacheng, Fang Shaomin, et al. Application Research of Personalized Mobile Learning Path Optimization Strategy[J]. Journal of Electrotechnical Education, 2016(1): 39-44.

[2]Zeng Ming, He Junjian.Design of Mobile Learning System in Universities[J].Software Guide,2015,14(9):87-89.

[3] Fan Xinmin. Analysis and Practice of Mobile Mobile Learning Security Protection Strategy [J]. Journal of Fujian Normal University (Natural Science Edition), 2018, v.34; No.159 (01): 17-22.

[4] Jia Runhong, Ji Guangping. The Necessity and Strategy of College Students' Mobile Learning in the Age of "Internet +"[J]. Journal of Huaihai Institute of Technology: Humanities and Social Sciences Edition, 2016, 14(10): 130-132.

[5] Li Guangjin. The Theory of "Mobile Learning" Theory Improvement [J].Journal of Heihe College, 2017, 8(2):86.