Universe Scientific Publishing

ORIGINAL ARTICLE

Analysis of Online Banking Risk Prevention Measures

Lingling Chen

Zhengzhou University of Aeronautics, Zhengzhou 450046, Henan, China.

Abstract: The advancement of technology and economic development have promoted the rapid development of online banking in my country. Especially with the rise of online shopping, online banking has become an indispensable part of people's daily lives. When people enjoy the efficient and convenient payment convenience of online banking, they are also at risk of network security. Banks should further update service systems, standardize internal personnel management, develop protection tools, and improve the security performance of online banking. Personal information should be protected and links and websites should be carefully opened when using personal online banking. Only when banks and users work together can the risk of using online banking is minimized.

Keywords: Online Banking; Risk Prevention; Measures

Online banking refers to a service system that uses a network platform to connect customer terminals to the bank's website, and finally realizes financial circulation. In recent years, with the rapid development of computer information technology, personal computers and mobile phones have gradually become popular, and online banking terminals are being widely used. The rapid economic development has promoted the formation of e-commerce, and personal online shopping has become an important part of people's lives. Internet banking has become an important way for people to transfer money, shop, and manage money. Compared with traditional banks, online banking has obvious advantages. Its advantages such as short transaction time, low cost, and high flexibility are popular, and its customer base continues to expand. In particular, the effective combination of online banking and e-commerce, and the electronic and digitalization of financial services have further facilitated people's lives and promoted the rapid development of the economy and society. As a virtual service method, online banking is highly technical, instantaneous, and open, which leads to higher risks than traditional banks. In recent years, personal property losses caused by the leakage of personal online banking information and the "hijacking" of personal computers or mobile phones have frequently occurred. More and more people have begun to pay attention to the safety and risk prevention of online banking.

1. The main risks of online banking

1.1 Technical risks

Technical risk is the core issue of online banking. It refers to the fact that in the promotion and use of online banking, the services provided cannot satisfy customers due to technical problems, or the back-end protection measures are not enough to be easily attacked by hackers, which leads to the interests of the bank and the interests of the bank. At present, online banking has technical risks in the four aspects of client security authentication, network transmission, system vulnerabilities, and data security. Once criminals have mastered the technical core of the above four aspects, the personal online banking system may be attacked by hackers at any time.

1.2 Manage risk

The management risks faced by online banking mainly include system emergency risks, internal control risks, and outsourcing management risks. Whether the bank has emergency response capabilities in system operation and maintenance, and whether it can guarantee the stability of system operation determines the existence of emergency risks. Whether the internal operation of the bank is smooth, whether the management

system is standardized, and internal personnel integrity issues determine the existence of internal control risks. When banks purchase third-party technical support, whether outsourcing services are not in place and whether there are confidentiality issues determines the existence of outsourcing management risks. The existence of management risks may cause the loss and disclosure of customers' personal information at any time, and endanger the rights and interests of customers.

1.3 Link risk

Linking risk refers to the risks that the e-commerce website cannot be linked to, customers cannot effectively distinguish the authenticity of the link, and it is easy to be used illegally duringthe transaction process of online banking. The existence of link risk provides convenience for criminals to conduct illegal activities. Because the link has a certain degree of concealment, users often click on it in the case of reluctance, which will eventually cause the leakage of personal information and cause losses.

1.4 User risk

User risk mainly refers to the user's low awareness of safety precautions, and criminals can take advantage of it. It is manifested in that users lack sufficient common sense of security, set their passwords too simplistically, or are too credulous in others, revealing their own account and password information to others. It is manifested in the lack of security awareness of users, using online banking at will in various occasions, or clicking links at will, or downloading and using applications at will, resulting in the disclosure of personal account information.

2. Bank online banking risk prevention

2.1 Update technical support in a timely manner

Online banking must establish good technical guarantees to ensure the smooth operation of the client's backend, protect user information, and protect the online banking system from "hacker" attacks. Banks should strengthen system security testing, regularly upgrade client systems, and continuously improve the security and stability of online banking systems by setting up firewalls, separating servers, and setting up high-security Web servers.

2.2 Strengthen staff training and supervision

On the one hand, we must strictly train business personnel, especially the training of professional ethics. On the other hand, it is necessary to standardize the management system, standardize the operation and management authority of the system, and clarify the division of labor. Finally, it is necessary to strengthen the inspection and supervision of audit, internal audit and supervision, discipline inspection and supervision departments, and establish a cyber risk audit center and risk early warning system when necessary.

2.3 Develop more and more practical user information protection tools

In order to ensure the security of user account passwords, various banks have developed various password protection tools, such as mobile phone dynamic passwords, dynamic soft keyboards, dynamic password cards, USB key certificates, etc., all of which are used to protect users' personal account information and avoid information leakage. To an important role. As an important means of protecting customer information, banks also need to research and develop safer and more practical protection tools.

3. Personal internet banking risk prevention

As far as personal online banking is concerned, technical risks and link risks are important reasons for the increasing number of victims. The following example uses case analysis to give examples of personal online banking risk prevention measures.

3.1 Prevention of typical phishing websites

Case introduction. In 2019, Liu had a number of mobile banking and online banking transfer transactions on his Agricultural Bank debit card, the amounts were 50 yuan, 500 yuan, 5,000 yuan, and 20,000 yuan. At first, Liu didn't care and thought it was at a certain time. Small consumption, but as the transaction amount increased, Liu began to have doubts. The party Liu and his family have not operated such transactions, but how did the online banking transactions occur? After investigation, it was discovered that Liu had previously logged into the fake website of the non-agricultural bank's official website due to the establishment of an online

banking business, which caused the bank card information to be intercepted by the website.

Case analysis. In online banking fraud cases such as fake websites, offenders often imitate formal online banking platforms to induce victims to perform online banking operations on false web pages, so as to obtain victims' online banking information and cash out the account amount.

Risk prevention measures. ① The network supervision department shall increase the monitoring of illegal websites, and promptly detect and close illegal websites. ② Banks should increase customer education. At present, online banking sites basically use digital certificates and special payment plug—ins. It is difficult for fake websites to do this. If banks increase their efforts to promote regular websites, Increasing customer education can prevent the infiltration of fake websites to a large extent. ③ Customers should be cautious when visiting websites and avoid logging in or browsing unhealthy websites, because such websites contain Trojan horses, which may monitor customer information at any time. At the same time, they should also pay attention to screening the website content and distinguish the authenticity of the website.

3.2 Typical online shopping risk prevention

Case introduction. Ms. Zhang received an unfamiliar phone call from a self—proclaimed store. The other party claimed that Ms. Zhang's online shopping had quality problems and needed to refund Ms. Zhang, and then sent Ms. Zhang a refund link. Ms. Zhang clicked on the refund link and filled in the account information, mobile phone number, account password and dynamic password as required. However, Ms. Zhang did not receive a refund for a long time and could not contact the "store".

Case analysis. Criminals make full use of the victim's fear of trouble and greed for cheap, by providing online shopping refund links, inducing the victim to fill in the refund information, so as to obtain the victim's payment information, and then through the Internet to achieve the purpose of cash withdrawal .

Preventive measures. ① Keep a clear mind at all times, and don't have the mentality of being convenient or greedy for petty gains. ② Be aware of official channels when handling online shopping, online returns, refunds, etc. ③ When applying for a refund or return on a shopping website, you must confirm the identity of the other party, and you should contact the official customer service before proceeding. Do not trust unidentified phone calls, online chat tools, or other informal network links. ④ Check carefully and do not disclose personal information easily. When receiving the dynamic verification code, carefully check whether the business type, transaction merchant, and amount in the SMS are correct. Don't easily disclose your ID number, bank card information, transaction password, dynamic verification code and other important information.

4. Conclusion

Nowadays, major banks have successively introduced detailed preventive measures regarding the security issues of online banking, such as strengthening short message service, strengthening certificate storage security, setting up dynamic password cards, providing advanced technology guarantees, implementing dual password control, and implementingtransaction limit control, increase transaction information prompts, run client—side password security testing, etc.

But even if the supervision of online banking continues to be strengthened, as long as the individual's awareness of prevention has not improved, the risk will not fade. Therefore, the most effective preventive measures are still individuals. As long as every online banking user keeps a clear mind, does not greedy petty gains, uses the online platform healthily, carefully clicks on links, carefully scans the QR code, and keeps his own identity information and account. Information, password information, etc. , criminals can't take advantage of it.

References

1. Peng Q, Pu Y. Risk analysis and prevention and control measures of my country's third—party payment. China Industry and Economics 2021; (9): 144—145.
2. Qian B. Exploration on the construction of payment risk control system under the new situation. China Credit Card 2021; (5): 6—8.
3. Hu B. Research on financial risk management of electronic banking based on sharing economy. Chinese Market 2020; (31):197—198.