Print

Commercial Online Banking Services Risk Assessment and Controls Evaluation

The Federal Financial Institutions Examination Council (FFIEC) has suggested that commercial online banking customers perform a related risk assessment and controls evaluation periodically. We are providing a template for your business to use as an exercise to ensure optimal security is in place. Please go through and complete the following steps and customize according to your business environment.

Date: _____

Responsible Person: _____

Business Name / Location: _____

Internet Based Financial Transaction Types (select all that apply)				
ACH ☐	Wire Transfer ☐	Merchant Services ☐	Remote Deposit ☐	Other ☐

Loss of financial transaction data and personally identifiable information is an inherent risk of using Internet based banking services. Protecting the confidentiality, integrity, and security of financial services transactions is shared by the Bank and the business entity. This Risk Assessment outlines some recommended security controls essential to minimizing the risk of these transactions for the business entity.

Consider the questions below and implementing suggested controls to mitigate the risk.

Controls in place to Prevent and Detect Fraud **Yes or No**	
Personnel Security:	
	1. Are your employees required to sign an acceptable use policy? *(If no, create an acceptable use policy and require your employees to sign it at least annually.)*
	2. Do employees who use Internet banking go through security awareness training? *(If no, require employees who use Internet Banking to go through security awareness training at least annually and at a minimum it should cover acceptable use policy, desktop security, log-on requirements, password administration guidelines, and social engineering tactics.)*
	3. Do you run background checks on employees prior to hire? (*Companies should have a process to verify job application information on all new employees. The sensitivity of a particular position or job junction may warrant additional background and credit checks. After employment, companies should remain alert to changes in employees' circumstances that could increase incentives for abuse or fraud.)*
Computer System Security:	
	4. Do computer systems have up-to-date antivirus software? (*Always, maintain active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.)*
	5. Is there processes in place to ensure software updates and patches are applied (e.g. Microsoft, web browser, Adobe products, etc.)? *(This includes a computer's operating system and other installed software (e.g. web browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc. In many cases, it is best to automate software updates when the software supports it.)*
	6. Is a firewall in place to protect the network? *(Use firewalls on your local network to add another layer of protection for all the devices that connect to the Internet through the firewall (e.g. PCs, smart phones, and tablets.)*
	7. Do you have an Intrusion Detection/Prevention System (IDS/IPS) in place to monitor and protect the network? *(An IDS/IPS is used to monitor network/Internet traffic and report or respond to potential attacks.)*
	8. Is your Internet Banking computer used to surf the web, email or visit social networking sites? *(The Internet Banking computer should be restricted from other Internet activity such as; email, web browsing, and social networking sites.)*
	9. Is Internet content filtering being used? *(If no, filter web traffic to restrict potentially harmful or unwanted Internet sites from being accessed by computer systems. For "high risk" systems, it is best to limit Internet sites to only those business sites that are required.)*
	10. Is e-mail SPAM filtering being used? *(If no, implement an e-mail SPAM filter to help eliminate potentially harmful or unwanted e-mail messages from making it to end users' inboxes.)*

	11. Are users of the Internet Banking system trained to manually lock their workstations when they leave them? *(Configure workstations to auto-lock after a period of inactivity along with training users to manually lock their work stations when they leave them. - Systems should be locked (requiring a password to reconnect) when users walk away from their desks to prevent unauthorized access to the system.)*
	12. Is wireless technology used on the network with the Internet Banking system? *(Wireless networks are considered public networks because they use radio waves to communicate. Radio waves are not confined to specific areas and are easily intercepted by unauthorized individuals. Therefore, if wireless is used, security controls such as encryption (WPA2 not WEP), authentication, and segregation are necessary to ensure confidentiality and integrity.)*
Physical Security:	
	13. Are critical systems (including systems used to access Internet banking) located in a secure area? *(Locate critical systems (including systems used to access Internet banking) in a secure area. - Only allow approved employees access to the critical systems.)*
	14. How are passwords protected? *(Ensure passwords are securely stored and kept confidential they should never be left out for unauthorized individuals to gain access.)*
Best Practices:	
	15. Do you always logoff Internet banking products when your computer is unattended or not in use? *(Leaving your Internet banking session signed in and unattended could allow anyone to gain access to your accounts either onsite or remotely.)*
	16. Do you vary your pattern of activity while using Internet Banking? (*Hackers rely on patterns of behavior to predict the best time to gain access remotely.)*