Online Banking for Business Accounts

Provided by
JACKSON COUNTY BANK
Member FDIC

Jackson County Bank, with guidance provided by the Federal Financial Institutions Examination Council ("FFIEC"), is providing this publication as framework for managing risks associated with Internet-based products and services (online banking). Because user awareness is a key defense against fraud and identity theft, an important part of online security is educating online banking customers about potential threats and safe practices. Those responsible for business banking accounts should have an understanding of the risks. By assessing the online risks on a periodic basis, your business can then evaluate and change the control mechanisms it uses in response to the changing threats to online banking activities.

Following are explanations of some of the risks, sound security practices, and your protections regarding online banking.

UNDERSTANDING THE RISKS

There have been significant changes in the online banking threat landscape, including rapidly growing organized crime groups, which have become more specialized in financial fraud and have been successful in compromising an increasing array of online controls. On an almost daily basis, internet users are warned about the latest scams, infectious spyware, or keystroke logging used by criminals who are seeking to profit illegally by taking over a business account, obtaining financial information, and stealing identities.

We realize that security is of great importance to you, and it has always been a priority at Jackson County Bank. That is why we have extremely high criteria to protect your banking information online. As a commercial online banking user, you should also use strong security practices and be alert to fraud and malware which could compromise your financial information, and lead to account take over.

DEFENDING AGAINST THE RISKS

Jackson County Bank has implemented ways to protect your information. To strengthen the Bank's existing vigilance, these layered methods of protection are reviewed and updated by assessing the risks as new information becomes available.

As an online banking user, it's important that you are aware of the current risks associated with online banking and practice sound security procedures as listed below to stay safe online.

LAYER YOUR SECURITY CONTROLS

High risk transactions, such as ACH (Automatic Clearing House), wires and online payments should especially use layered controls to combat risks.

Suggested effective controls included in a layered security program include, but are not limited to:

- the use of dual authorization through different access devices;
- the use of out-of-band verification (fax, phone, text, etc.) for transactions;
- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
- enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows;
- internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels.

FFIEC RECOMMENDATIONS FOR BUSINESS ACCOUNTS

- ➪ Business account holders are urged to conduct periodic assessments of their internal controls.
- ➪ Layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations.
- ➪ Initiate enhanced controls for high-dollar transactions.
- ➪ Increase your security controls as the dollar amount of your transactions increase.
- ➪ Use multi-factor authentication (MFA). MFA uses combinations of authentication to identify a user. These may include something he knows, such as password/PIN, something he has, such as a token or certificate, and something he is, such as biometrics.

IF YOU HAVE SUSPICIOUS ACTIVITY

Never share personal information unless you are confident of who you are dealing with. Jackson County Bank will NEVER send unsolicited e-mails or call asking customers to provide, update or verify passwords or PINS, credit or Debit card numbers or Social Security numbers.

If you have questions or concerns regarding a questionable e-mail, telephone call, an unauthorized transfer, or other suspicious activity please contact us immediately at:

Jackson County Bank
8 Main St., P.O. Box 490
Black River Falls, WI 54615
(715) 284-5341

jcbank

JACKSON COUNTY BANK
Black River Falls, Alma Center, Hixton, Merrillan, Taylor
Member FDIC Phone (715) 284-5341
jacksoncountybank.com

USE THE CHECKLIST BELOW TO SELF ASSESS YOUR BUSINESS SECURITY PRACTICES

□ Use a dedicated computer for your ACH or online transactions. Do not use this computer for e-mail or browsing the Internet. Malicious software often gets into systems through activities such as web surfing or reading e-mail. Using a computer exclusively for your online transactions goes a long way toward increasing security and reliability.

□ Install, run and keep anti-virus and internet security software updated. Virus protection and internet security programs require regular updates to keep your computer protected against newly discovered threats. It is very important to keep the subscription active for this protection. Most programs have an automatic update feature. Make sure this is turned on and set to check for new updates and to scan your computer regularly.

□ Install firewall software or hardware. Most anti-virus and internet security products now bundle in firewall software with their products. Installing "free" virus protection software may not be protecting you completely, and you may find the cost of the total protection software pales when compared to the cost of repairing your computer—or your reputation!

□ Protect your computer by keeping your operating system patched. These are updates that can patch "holes" in the operating system security through which some malicious programs or viruses could attack. Turn on automatic updating to ensure the updates are being applied.

□ Be sure to perform updates on other software on your computer also, including, but not limited to your Internet browser, Adobe products, Java, SQL and other third party software. These updates often include security enhancements.

□ Use unique user IDs and complex secret passwords to access programs, websites and computer systems. Use a long passphrase instead of a password. For instance, use the first couple of letters in each word of a song, rhyme or phrase, then add in numbers and symbols for complexity.

□ Do not share your passwords, nor use the same password for different applications. If you must write down passwords, store them securely.

□ Be sure a password has been set up to log onto the computer. The computer should be properly locked any time the workstation is unattended; and log out if away for an extended time period and at the end of each day. Turn on an automatic password protected screensaver after 15 minutes or less. Turn your computer off when not using it. Change passwords frequently. A recommended policy is to change passwords at least every 40 days, and not reuse passwords within ten changes.

□ Be sure to close the browser completely when you log out of your banking software, or any other secure website.

□ Disable the feature on your browser that allows user names and passwords to be saved.

□ Never use a public computer for ANY type of banking transactions; nor should you use public Wi-Fi.

□ A wireless Internet connection is not recommended.

- However if you must use a wireless connection, be sure that your access point or router has the current security capabilities. If your access point is older than 2 or 3 years old, it probably isn't capable of the latest security protocols and should be replaced.
- When configuring the access point or router, change the default passwords to complex unique passwords and also change the default network name (SSID). Enable the firewall on the access point.
- Position your wireless access point in a place where it is least likely to leak outside your location, such as the center of your building.

□ Avoid downloading files from the Internet. Many times malware can be piggy-backed with legitimate software. Other times websites or alerts may "scare" you into downloading software, advising you that you have a virus and you must download software immediately to take care of it. This is called "scareware", and may install a Trojan or other malware on your computer.

□ Protect your answers to security questions. Select questions and answers that are easy for you to remember, but hard for anyone else to guess. Use questions that someone could not answer by looking in your wallet or on a social networking site. Do not write the questions or answers down or share them with anyone.

□ Do not use flash drives, DVDs, smart phones or other portable drives on your banking or business computer. All these devices have the potential to introduce malware to your computer.

□ Never send any type of banking or confidential information by e-mail, messaging or social networking site. Only send this information on properly secured and encrypted known sites when necessary, or via secure e-mail.

□ E-mail is one of the most common sources of malware. If you must use e-mail on your banking or business computer:

- Refrain from clicking on links in e-mail messages. Instead type the known address of the site into your browser, and locate the content from there.
- Be careful of suspicious e-mails. Never open attachments, click on links or respond to e-mails from unknown senders. Do not open unexpected attachments even if they come from trusted sources.
- Turn off the preview pane for all e-mail folders. The preview pane may actually activate malicious code in an e-mail.

□ Store security tokens securely. If you use tokens, make sure they are not accessible to others. Never give out the token serial number unless required by a known employee of your bank.

□ Set enhanced controls over account activities. If you are able, set limits on transaction value thresholds and computer IP address restrictions, for example.

□ Always use an "out-of-band" confirmation tool that would be unknown to a fraudster to validate your ACH transactions.

□ Use Dual Control prior to initiating ACH or wire transactions. Add security by requiring dual verification of files prior to submission to the bank.

□ Train all employees on information security. In addition to annual training, use a process to regularly identify risks and controls for changing internal and external threats.

□ Remove exiting employees from your system immediately. Set up a procedure for removing exiting employees as users on bank related platforms, websites, e-mail and computers.

□ When disposing of equipment, properly clean drives or destroy equipment. Simply deleting files or formatting drives is not sufficient.

Protections Provided for Electronic Funds Transfers under Regulation E

Regulation E and the federal Electronic Fund Transfer Act afford protections **only to individual consumers and do not include business/commercial organizations**. Regulation E, under the Electronic Fund Transfer Act, provides a framework that establishes the rights, liabilities, and responsibilities of those participating in electronic fund transfers such as ATM transfers, bill payment services, point-of-sale transfers in stores, and preauthorized transfers including direct deposit and Social Security payments.

You must notify Jackson County Bank AT ONCE if you believe an unauthorized electronic funds transaction involving your business account has been made. Notify us AT ONCE when your online banking credentials or security tokens have been used without your permission. You will be liable for any and all unauthorized transactions that occur through online banking. You are responsible for maintaining procedures to protect online banking credentials and security tokens including common PC security measures. It is your responsibility to notify Jackson County Bank IMMEDIATELY when an employee who uses online banking on behalf of your business is terminated or his/her responsibilities no longer require online banking access. Jackson County Bank shall be liable only in the event of loss due to its gross negligence or willful misconduct.

EDUCATE YOURSELF

As an online user, understanding the current threats and knowing how fraudsters may steal your information is critical. Visit our website at jacksoncountybank.com for information and online security tips.

For more information regarding online safety and security visit:

www.ftc.gov
Federal Trade Commission

www.staysafeonline.org
National Cyber Security Alliance

www.ftc.gov/idtheft
FTC Identity Theft Site

www.antiphishing.org
Anti-Phishing Working Group

www.nacha.org/Fraud-Phishing-Resources
NACHA, The Electronic Payments Association

JACKSON COUNTY BANK Member FDIC
March, 2014