Online Banking for Consumer Accounts

Provided by
JACKSON COUNTY BANK
Member FDIC

FFIEC ISSUES NEW GUIDANCE

On June 28, 2011, the Federal Financial Institutions Examination Council ("FFIEC") published the Supplemental Guidance on Internet Banking Authentication to help financial institutions make online transactions safer and more secure. 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. 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 obtaining and using your financial information or identity.

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 an online banking user, you should also use strong security practices and be alert to fraud and malware.

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 Internet 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.

STAY SAFE ONLINE

- **Keep security software current.** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Automate software updates for your anti-virus, spyware, operating system and other third-party software. Protect all devices that connect to the Internet including smart phones, gaming systems, and other web-enabled devices. Use a firewall with your computer. Most anti-virus and anti-spyware products now bundle in firewall software with their products.

- **Protect Your Personal Information.** Refrain from giving out your personal information unless it is absolutely necessary. Think before you give out your social security number, mother's maiden name, email address or other information. Never email confidential information.

- When dealing with financial service providers, inquire about their security practices. Many businesses offer additional security options or ways for you to verify who you are before you conduct business on their site.

- If you use security questions and answers for secure websites, select questions and answers that someone else could not find in your wallet or on a social network, or simply guess.

- **Make passwords long and strong.** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
Use separate passwords for every account and change these passwords frequently to help thwart cybercriminals.

- **Adjust security settings on your computer.** When available, set the privacy and security settings on browser or websites to the highest level of security that will function with the application. Disable the feature on your browser that allows usernames and passwords to be saved. Be sure to close the browser completely when you log out of your banking software, or any other secure site.

- **Open with Caution.** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete. Fraudsters often capitalize on your curiosity, offer you great deals, or attempt to scare you, to get you to click and download malware.

- **Connect with Care.** Do your internet banking activities on secure computers only. Public computers (internet cafes, hotels, restaurants, etc.) or public Wi-Fi should not be used for any type of banking transactions.

- If you use a wireless internet connection in your home, be sure your router is current enough to be capable of the newest security features. Configure your router with a unique password and change the default network name (SSID). Enable the firewall on the device, and position it in a place where it is least likely to leak outside your home.

- When banking and shopping online, check to be sure the site is "security enabled". Look for a lock on the browser, or web addresses with "https" or "shttp". Even if it appears to be a secure site, it's important that you know who you are doing business with. Be sure that the business also uses secure methods to store your personal information after is delivered over the internet.

- Do not allow someone else to use a flash drive, DVD, or other portable device with your computer unless you know it is free from malware.

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 emails 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 email, 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

YOUR PROTECTIONS UNDER REG E

Liability of consumer for unauthorized transfers:

Regulation E, under the Electronic Fund Transfer Act (EFT), provides a framework that establishes the rights, liabilities, and responsibilities of those participating in EFT such as ATM transfers, bill payment services, point-of-sale transfers in stores, and preauthorized transfers including direct deposit and Social Security payments. Regulation E covers an individual consumer who authorizes a financial institution to electronically transfer funds to debit or credit his/her account.

If you are an individual and your account was established for personal, family or household purposes, notify Jackson County Bank AT ONCE if you believe an unauthorized electronic funds transaction involving your consumer account has been made or your Internet Banking PIN or Internet Banking User ID have been used without your permission. You can lose no more than $50.00 if you tell us within two business days*. If you DO NOT tell us within two business days after you learn of the unauthorized transaction, loss or theft of your Internet Banking PIN or Internet Banking User ID, and we can prove we could have stopped someone from using your Internet Banking PIN or Internet Banking User ID without your permission if you had told us, you could lose as much as $500.00. Telephoning is the best way of keeping your possible losses down; however you may notify us in person, by telephone, or in writing.

If you do not tell us about an unauthorized transaction, within 60 days of the date we mail a periodic statement to you, you may not get any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip or a hospital stay) kept you from telling us, we will extend the time periods.

If you believe your Internet Banking PIN or Internet Banking User ID has been lost or stolen, or that someone has transferred or may transfer money from your account without your permission, call us at 715-284-5341 or write to us at P.O. Box 490, Black River Falls, WI 54615-0490.

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

*For purposes of this notice, our business days are Monday thru Friday. The following holidays are not included as business days: Christmas, New Year's Day, Labor Day, Memorial Day, Thanksgiving Day and Fourth of July.

January, 2012