

April 2010	 Bank of Central Florida	Treasury Management
		Volume 2, Issue 1

BEST PRACTICES

1. SOFTWARE PATCH UPDATES

Verify that all currently available security patches are installed. You may decide to make exceptions for patches that compromise the usability of critical applications.

2. ANTI-VIRUS SOFTWARE

Anti-Virus Software should be running and up-to-date at all times.

3. FIREWALL SOFTWARE

Connecting to the Internet can pose dangers to unwary computer users. Use a firewall to help reduce your risk.

Installing a firewall is just one step toward safe surfing online. You can continue to improve your computer's security by keeping your software up to date, using anti-virus software, and using antispyware software.

4. PASSWORDS

Here are some tips for making your passwords more secure. The more secure a password, the less likely someone will be able to "crack" it. Using password safety, choose a password with the following criteria:

- At least 8 characters in length
- At least 1 number
- At least 1 special character like & or *
- Both upper and lowercase characters

Passwords with difficult combinations make it harder for password cracking tools to figure out your password.

Don't use personal information such as birthdays, children's names, or first and last names when creating a password. Avoid using words or phrases that could be found in a dictionary or easily guessed.

5. KEEP INTERNET BROWSER UP-TO-DATE

Hackers also take advantage of Web browsers (like Firefox or Internet Explorer) and operating system software (like Windows or Mac's OS) that don't have the latest security updates.

In addition, you can increase your online security by changing the built-in security and privacy settings in your operating system or browser. Check the "Tools" or "Options" menus to learn how to upgrade from the default settings. Use your "Help" function for more information about your choices.

If you're not using your computer for an extended period, disconnect it from the Internet. When it's disconnected, the computer doesn't send or receive information from the Internet and isn't vulnerable to hackers.

6. PHYSICAL SECURITY

Unauthorized physical access to an unattended computer can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, consider configuring your computer to "lock" and require a user to re-authenticate if left unattended for more than a certain amount of time.

7. LEARN WHAT TO DO IN AN E-EMERGENCY

If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information. Malware could be sending your personal information to identity thieves.

Confirm that your security software is up-to-date, and then use it to scan your computer. Delete everything the program identifies as a problem. You may have to restart your computer for the changes to take effect.

If the problem persists after you exhaust your ability to diagnose and treat it, you might want to call for professional help. If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem. Your notes will help you give an accurate description to the technician.

If you need professional help, if your machine isn't covered by a warranty, or if your security software isn't doing the job properly, you may need to pay for technical support. Many companies, including some affiliated with retail stores, offer tech support via the phone, online, at their store, or in your home. Telephone or online help generally are the least expensive ways to access support services, especially if there's a toll-free helpline, but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a technician or repair person to come into your home.

Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do to avoid it in the future. Also, talk about safe computing with anyone else who uses the computer or network.

While banks consider online banking security solutions, customers are increasingly faced with choices about their own use of these systems as they exist today. Some suggest stand-alone computers running open source operating systems as a security measure. Bank customers can make further use of "positive pay" arrangements with the bank and can monitor their account activity daily.

Specific Recommendations for Bank of Central Florida ACH Origination Clients:



Dual Release

One person submits for approval and the second reviews and transmits the file. It is best if submitting user is not the admin user.

Pre-note delay

This requires a new detail entry to be added to the template X number of days prior to the “live” dollar value entry initiation. At least 2 days prior is recommended. Note that in order to verify the validity of the new account number and routing, the pre-note must be initiated 6 days prior to the “live” date. The pre-note will be automatically generated once a new detail entry is added to the template. The number of delay days is maintained at the bank level and, therefore, cannot be changed by the unauthorized user.

Account Alerts for template changes

Activate the account alerts in the communication section of administration. An email alert will be sent when the template changes. Should an email be received for a change that was not initiated by an authorized user then additional research should occur immediately. Notify Treasury Management if the change is not authorized.

Appropriate Batch Limits

A normal batch limit should be in place in the ACH system on Business Internet Banking. If an occasional higher amount is required, the higher amount will be pre-approved and then added to your profile via an email or phone call to Treasury Management. This limits the exposure on the system.

Daily monitoring of all account activity for unusual or unauthorized activity

Review all checking activity daily and report any suspicious transactions to Treasury Management or your Relationship Banker immediately.

Monitor the ACH History for accuracy

Pint out your confirmation and review the batches in the queue before and after the initiation of a new batch.

Up-to-date Virus Protection Software and Firewalls

Make sure that the virus software is the latest version and updated on all computers in your office(s).

Email Policy

Initiate an email policy that prohibits the opening of unknown senders’ emails and attachments. Ensure employees know the potential of a virus, sent by a fraudster, infecting their computer through a seemingly innocent attachment to an email.

Check off the steps that you are following for your company’s security in the ACH online origination module. Can you add to your secure environment? Only you know for sure that the activity is correct and that your computer is operating in a safe environment.

For additional information on implementing steps outlined above please email Nancy LaFountain in Treasury Management at nancy.lafountain@bankofcentralflorida.com or call 863-904-4122.