

Online Transaction Precautions

Take Steps to Mitigate Risk

Daily Functions & Responsibilities...

- ✓ Ideally, establish a stand-alone PC with a clean hard-drive with the sole function to do online banking and card purchases on secure web sites. The PC should be configured that it may not receive e-mails nor be able to visit any sites other than authorized secure sites and should not be on the same network as the rest of the organization.
- ✓ Limit administrative rights on users' workstations. This will help prevent the inadvertent downloading of malware or other viruses by users.
- ✓ Locking the workstation ensures that unauthorized users may not gain admittance to computers when left alone.
- ✓ Dual-control functions provide protection and accountability for your employees. For example, one employee may have authority to prepare ACH files (such as payroll) while another must send them.
- ✓ Backup files and store them in a secure place, such as a safe or safe deposit box.
- ✓ Logoff at the end of the day.
- ✓ Keep anti-virus and anti-spyware tools continually updated and run regular system scans.
- ✓ Review account activity DAILY.



Passwords...

- ✓ Password protect all office computers.
- ✓ Assign individual Usernames and Passwords. Common passwords reduce accountability and make it difficult to trace fraudulent activity. Employees who leave the company may continue to have access to tools and services with common passwords.
- ✓ Do not share passwords.
- ✓ Do not write down passwords.
- ✓ Do not use the "Save Password" feature on login forms.

Former employees may be another potential vulnerability. When an employee leaves your company, here are a few measures you will want to consider:

- ✓ Deactivate all computer accounts immediately.
 - While online tools are convenient, many may be accessed outside of the office (such as from home or a public computer).
 - We suggest you deactivate instead of delete, because, in many cases, deleting users erases all records of their activity. Access to such information may become necessary.
- ✓ Repossess keys, access cards, parking passes, etc.
- ✓ Change any door key codes or common passwords (which we hope you have eliminated by this time)

For further information on securing your office, feel free to use the resources listed below:

<http://www.microsoft.com/security/default.mspx>
<http://onguardonline.gov>
<http://www.fdic.gov>
<http://www.ftc.gov/acoas/index.htm>

For more information on National Exchange Bank & Trust business services, please contact:
Business Services Group | 920.921.7700 | businessbanking@nebat.com

