TB&T Suggestions / Best Practices for Protecting Your Company

Management Level

- Implement Dual Control procedures
- Implement and continually reinforce a Data Security Awareness program. Education is key – training of employees cannot be overemphasized. And we have a new way of helping you do this!
- Establish audit procedures to ensure compliance with data security policy as well as to ensure no financial malfeasance; reconcile bank accounts daily
- Make sure that your employees know how and to whom to report suspicious activity to at your company & at TB&T (Shane Greeley 260-2119; Tim Murphy 260-4145; Anna Jones 260-2118)
- Choose your administrator carefully; consider being administrator yourself (as owner or executive); if not, then dictate parameters in writing to administrator (limitations, dual control, etc.)
- Limit administrative rights in TB&T Net Teller, through which you can set limits by user for:
    - Access time of day
    - Per wire limit
    - Dual wire control and/or dual wire control limit
    - Daily ACH limit
    - ACH upload, edit, initiate or delete
    - Transfer limit between accounts
    - NetTeller rights:
        - View current balance
        - View statements
        - Enter stop payments
        - Modify / delete wire
- Administrator can also designate authorized IP addresses from which transactions can be initiated
- Administrator can also set up email alerts based on various criteria.
- Call us if you have any questions about managing your risk through NetTeller
- Review and understand roles and responsibilities under your TB&T cash management agreement
- Considering having a dedicated computer for banking transactions only
- Consider outsourcing network management and IT security function if you do not have internal expertise. It is important to stay abreast of changing security trends and cybercriminal tactics.

IT Level

- Secure your computers and networks
- Install and maintain spam filters
- Install & maintain real-time anti-virus & anti-spyware desktop firewall & malware detection & removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
- Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices.
- Install security updates to operating systems and all applications as they become available.
- Limit administrative rights for your networks; do not allow employees to install any software without receiving prior approval.
- Restrict internet usage / sites. White list sites as needed.
- Block pop-ups

User Level

- Use long and complex passwords and change them frequently
- Never write your password anywhere it can be observed by others
- Avoid using bank password with other applications.
- Never provide information regarding your token.
- Protect Tokens, Log-in IDs and passwords (most often found in lap drawer or under keyboard)
    - Don't write down, but if you do, keep on person and/or encrypt (e.g, *TrueCrypt*)
    - Tokens – lock up or carry on key ring
- Always lock your desktop when stepping away from your computer.
- Always log out of TB&T NetTeller and close your web browser when you are finished.
- Surf the internet carefully
- Do not open attachments from e-mail; be on the alert for suspicious emails (see next page)
- Do not use public internet access points, especially for accessing bank accounts.
- Note any changes in the performance of your computer - dramatic loss of speed, computer locks up, unexpected rebooting, unusual pop-ups, etc.
- Be suspicious of emails or calls requesting your user name, token information, or passwords.
- TB&T will never request your password or your token information via email
- Contact TB&T if you:
    - Suspect a fraudulent transaction
    - If you are trying to process an Online Wire or ACH Batch & receive a maintenance page.
    - If you receive an email claiming to be from TB&T and it is requesting personal or company information.

E-mail Usage:

- Some experts feel e-mail is the biggest security threat of all.
- What may be relied upon today as an indication than an email is authentic may become unreliable as electronic crimes evolve.
- The fastest, most-effective method of spreading malicious code to the largest number of users.
- Also a large source of wasted technology resources
- Examples of corporate e-mail waste:
    - Electronic Greeting Cards
    - Chain Letters
    - Jokes and graphics
    - Spam and junk e-mail

Warning Signs of Potentially Compromised Computer Systems

- Inability to log into online banking (thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money);
- Dramatic loss of computer speed;
- Changes in the way things appear on the screen;
- Computer locks up so the user is unable to perform any functions;
- Unexpected rebooting or restarting of the computer;
- Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.);
- New or unexpected toolbars and/or icons; and
- Inability to shut down or restart the computer.