

Safe Computing Practices

Security Tips for Companies That Bank Online

While it is your responsibility to safeguard your own data, including information that can be used to access or transact against your accounts at Capital One, National Association, we recommend that you consider implementing the following data security-related rules or controls for your company:

Best Practices for Online Banking Security

- Use strong, complex passwords that contain:
 - alpha/numeric characters and symbols
 - upper and lower case characters
 - minimum of 8 characters but longer is recommended
 - no real words or names of family/friends/pets
 - use entire keyboard; avoid strings of identical characters
- Change your password regularly and never use your online banking password on another Web site.
- Never reveal your confidential login ID, password, PIN or answers to security questions to anyone.
- Never reveal your confidential login ID, password, PIN or answers to security questions by e-mail.
- Never share your security token.
- Report lost or stolen tokens immediately.
- Never bank online using computers at kiosks, cafes, unsecured computers or unsecured wireless networks.

Tips to Avoid Phishing, Spyware and Malware

- Don't open e-mail from unknown sources.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail:
 - Call the purported source if you are unsure who sent an e-mail.
 - If an e-mail claims to be from your bank, call a client services representative.
- Educate your staff about current scams and loss-prevention steps.
- Make sure all of the computers your staff members use for work-related business — at the office and at home — have the latest versions and patches of both anti-virus and anti-spyware software.
- Maintain updated and patched systems and software.
- Install a firewall between your computers and the Internet.

- Restrict administrative rights to install programs to IT staff.
- Check your settings and select at least a medium level of security for your browsers.

Tips to Protect Online Payments & Account Data

- Dedicate and restrict one computer to online banking transactions; allow no Internet browsing or e-mail exchange and ensure this computer is equipped with latest versions and patches of both anti-virus and anti-spyware software.
- Segregate responsibilities among different employees by maintenance, entry and approval.
- Delete online user IDs as part of the exit procedure when employees leave your company.
- Assign dual system administrators for online cash management services.
- Periodically evaluate employee job functions and remove online services.
- Establish transaction limits for employees who initiate and approve online payments.
- Set up alerts to notify manager of payments initiated above a threshold amount that warrant management's attention.
- Use dual controls; require multiple users to release an online payment because it is less likely a fraudster would control the workstation of both initiating employees.
- Reconcile by carefully monitoring account activity and reviewing all transactions initiated by your company on a daily basis.
- Use separate accounts for electronic and paper transactions to simplify monitoring and tracking any discrepancies.

There is no substitute for the advice of experts with intimate knowledge of your operations. We at Capital One, National Association recommend that you obtain data security and anti-fraud advice from such experts. While we may provide you with some recommendations regarding controls or best practices from time to time, these recommendations cannot replace the services of dedicated data security and anti-fraud experts with a true understanding of your business.

If you suspect you may have been a victim of a fraudulent online banking scam regarding your Capital One Treasury Optimizer® or TowerNET™ service, contact Capital One Treasury Management Client Services: Treasury Optimizer® (NJ & NY) call 1-866-632-8888 or TowerNET™ (LA & TX) call 1-888-822-2274.

To report a phishing e-mail, forward the e-mail to abuse@capitalone.com.
To learn more, click on the Security link at the bottom of every CapitalOneBank.com Web page.
For a copy of this document, go to www.capitalonebank.com/safecomputing.