

BANKING SAFETY TIPS

Do you use your laptop at the airport? . . . Here are some safety tips:

WiFi Connections...There may be hacker danger for business travelers connecting to a wireless internet connection at a public place, like at an airport. Here are some safety tips from the Better Business Bureau:

- Never connect to an unfamiliar “ad hock” network, even if the name sounds genuine. A hacker can change the name of his/her network to anything, including the name of the legitimate Internet connection offered by the airport. Just because the network is using the same WiFi name advertised in the airport, don’t believe it.
- Make sure your computer is not set up to automatically connect to non-preferred networks; your computer could automatically connect to the hacker’s network without your knowledge.
- Turn off file sharing when you are on the road so hackers cannot steal entire documents, files and unencrypted email from your computer.
- Create a virtual private network or VPN for your business; a VPN establishes a private network across the public network so that nobody in between can intercept data.

Learn more at this Better Business Bureau Website:

<http://www.bbb.org/alerts/article.asp?ID=770>

Do you know the most common online dangers and how to protect yourself?

- Phishing...fraudulent emails that try to copy cat your bank or similar trusted sources. *Never respond with any personal information to “verify” anything they ask.*
- Pharming...Intercepted Internet traffic re-routed to a fraudulent site where you are asked to enter personal information – *Never respond with any personal information.*
- Mailware...Software that infiltrates or damages your computer system without your knowledge (viruses, worms, Trojan horses, spyware and adware. **Always keep your anti-virus protection up to date.**

Your Bank Keeps You Protected in Many Ways:

- Passwords and Pins...use mixture of numbers and letters and never share!
- Multi-factor Authentication...multiple forms of ID and secret questions before you can access your account.
- Encryption...software that converts information into code, readable by only you and your bank.

- Privacy Policies...keeping your information secret and secure per federal and state mandates.

More Safety Steps You Can Take:

- Keep your anti-virus protection current.
- If you receive suspicious, unsolicited email from your bank, call them first before opening it to make sure it truly came from your banker.
- Always log off any site properly after conducting any personal banking, bill paying, utility, or credit card personal online transactions.
- Never respond to any unsolicited or suspicious request for any type of personal information. (Remember, your bank already received all the information they need on you when you first opened your account.)

Learn more about protecting yourself, your money, and your identity from these financial industry regulators:

Federal Deposit Insurance Corp.: <http://www.fdic.gov>

Board of Governors of the Federal Reserve System: <http://www.federalreserve.gov>

Office of the Comptroller of the Currency: <http://www.occ.treas.gov>

Office of Thrift Supervision: <http://www.ots.treas.gov>

Federal Trade Commission: <http://www.ftc.gov>

...or feel free to email us at info@eaglebankmd.com ("Attention Security and Compliance") or call or visit your local EagleBank office.

The safety tips above were extracted from various banking industry publications and security materials. For complete details and more information, visit the web sites listed above and throughout these tips.

