PINNACLE BANK
REACH HIGHER

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clinking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.
- 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 claiming to be from your Bank seems suspicious, checking with your Banking contact may be appropriate.
- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Update all of your computers with the latest version and patches of both anti-virus and anti-spyware software.
- Ensure computers are patched regularly, particularly operating systems and key application with security patches.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Check your settings and select, at least, a medium level of security for your browsers.
- Clear the browser cache before starting an internet banking session in order to eliminate copies of the Web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browsers preferences menu.