SECURITY TIPS!

Colonial Federal Savings Bank utilizes multiple layers of security to protect your personal and account information. As our customer there are things you can also do to protect yourself.

Beware of:

- Unsolicited "Phishing" attempts to obtain personal information which can be used to assume your identity. You should never provide personal information to anyone, even if the request appears to be from a company you may know. If you are uncertain who the request is from or what they will do with your information, always contact them directly before you respond.

- Pop-Up screens requesting personal or login information after you log into an online system. Malware on your computer can sense you accessing secure financial sites and may trigger the popup in an attempt to obtain your login credentials and other personal information. **If an unsolicited pop-up appears do not complete the form.**

- "Spoofing" of web pages that request personal data such as account number, social security number, ATM card, PIN or credit card information. A spoofed web page may look like a legitimate financial site, but it is actually a fraudulent site attempting to obtain your personal information. Always use your own links to sites or type the web address yourself. If you don't see your usual security features on the site (i.e. your picture and phrase), do not proceed.

Business owners:

Perform a periodic risk assessment of your access devices to ensure they are secure and up to date with all mitigating security measures (i.e. patches, anti-virus signatures etc.). Risk assessment forms can be obtained by emailing service@colonialfed.com. We strongly recommend you review your accounts daily, as this is the quickest way to detect fraud. Online Banking, including mobile access and account alerts, is available to our business customers.

All Customers:

Colonial Federal Savings Bank will NEVER ask you for any personal information (account numbers, passwords, PINs, social security numbers, etc.) through an unsolicited automated phone call, e-mail or unusual web page. If you receive an unsolicited request, do not provide this information and call us directly at 617-471-0750.

We use SSL encryption on our website, which is just one of the multiple security layers in place to help protect your confidential information. Internet security, however, does not rely on technology alone. You must also be on alert for spyware, viruses, and computer hackers and not become a victim of social engineering.

We highly recommend you take the following Steps to Protect Yourself:

- **Act quickly if you suspect fraud:** If you believe someone is trying to commit fraud and/or if you think you may have provided personal or account information in response to a fraudulent email or Web site, report the incident immediately, change your passwords and monitor your account activity frequently.
- **Keep your computer up to date with the latest patches for known vulnerabilities:** For Windows users, open your browser, and go to "Tools." Click on "Windows Update," and follow the instructions to download the latest patches.
- **Make sure your computer has the most current security and anti-virus software and run scans regularly:** Anti-virus software needs frequent updates to guard against new viruses. We recommend that you use a program that automatically updates your virus protection daily. If you currently do not have this automatic update feature, we suggest you upgrade to a new virus detection program.

- **Run anti-spyware software frequently:** Many anti-virus software packages can detect adware/spyware programs on your computer. If your anti-virus software doesn't include spyware detection, we recommend you install comprehensive spyware detection. If found, spyware should be removed immediately. (Pop-up ads can indicate that adware/spyware is running on your machine.) Spybot, an award-winning software program, can be downloaded for free at safer-networking.org
- **Install a firewall to prevent unauthorized access to your computer:** Firewalls are an important security measure, especially if your computer is left on or unattended.
- **Monitor your credit report:** Your can obtain a free credit report annually from each of the three major reporting agencies at annualcreditreport.com. As each agency will only provide one free report in a 12 month period, we recommend you request your report from a different agency every 4 months.
- **Review Credit Reports for your children:** Help your children get into the habit of monitoring their credit reports when they reach their teens. Children are targeted as much as 35 times more frequently than adults, because using a child's ID allows fraudsters more time to go undetected. Social Security numbers stolen from schools, doctor's offices and hospitals can go undetected for years, resulting in bad debt which parents may be responsible for.
- **Exercise caution when traveling:** Make sure your laptop or device is updated with the latest patches prior to leaving home. Don't install updates or patches on your computer or device while using a hotel or public WiFi service.
- **Logoff Online Banking before leaving your computer or device**: When your computer is not in use, shut it down or disconnect it from the Internet
- **Review your account history frequently:** If you detect any unauthorized activity, contact us immediately at 617-471-0750.
- **Add a PIN or password to mobile devices:** Your mobile device is full of personal information. By enabling PIN or password security and also using the remote wipe function, your information will remain safe if your device is lost or stolen.
- **Use complex passwords:** Your password should be at least eight characters long including numbers, upper and lower case letters and at least one symbol. Passwords should be changed frequently. We recommend using a different login and password for your financial account logins.
- **Be alert for scam emails:** These may appear to come from a trusted business or friend, but actually are designed to trick you into downloading a virus or linking to a fraudulent website and disclosing sensitive information. Look for misspellings in the email, especially business names and links to websites.
- **Open emails only when you know the sender:** Verify the spelling of the senders name and be especially careful opening an email with an attachment. We advise against opening attachments unless you are confident that you can trust the source.
- **Send personal or financial information only by encrypted email or on a secure website:** Regular emails are not encrypted and are more like sending a post card; anyone can read it. To ensure that SSL encryption is protecting your private communication, look for the URL prefix "HTTPS" at the beginning of the address bar. Also look for your specific web browsers SSL icon.
- **Protect your social media identity:** Your social media ID can be more valuable than your credit cards. Take precautions to protect your social ID; if you stay logged in on your mobile device make sure you secure your device with a password.

Additional resources for help and information include:

Financial Fraud Enforcement Task Force: stopfraud.gov
Federal Trace Commission (FTC) Consumer Response Center: ftc.gov
Consumer Guides and Protection: usa.gov
Internet Crime Complaint Center: ic3.gov