ARUNDEL FEDERAL
SAVINGS BANK

BE SAFE AND SECURE IN THE ONLINE WORLD

SAFE COMPUTING TIPS

Install or Update Your Antivirus and Antispyware Software:
Antivirus and Antispyware software are designed to prevent and detect malicious software programs on your computer. In order to keep your computer and your identity safe all computers connected to the internet for any length of time should have both of these products installed at all times.

Run a Full Scan With Both Your Antivirus and Antispyware Software:
Full scans with your Antivirus and Antispyware software can help to catch the most recent viruses and spyware that may have been installed on your computer without your knowledge. Full scans of your entire PC should be run at least daily.

Ensure Your Operating System is Up to Date:
Computer operating systems need to be updated to stay current with any security patches released by the maker of your operating system. Visit your operating system (Microsoft, Apple or other) and browser's web site (Chrome, Internet Explorer, Safari, Firefox, etc.) frequently to make sure that the most recent updates are installed.

Keep Your Software Up to Date:
In addition to keeping your operating system up to date you should also look for updates for the software installed on your PC. This includes software such as Adobe products, Java, Firefox, and Apple iTunes. Software such as this can be vulnerable to hacker attacks and may lead to the compromise of your system if it isn't updated. A good rule of thumb is that if you don't need a piece of software don't install it or remove it when it is no longer needed.

Keep Your Firewall Turned On:
A firewall helps protect your computer from hackers who may try to gain access to your computer and the information it contains. Software firewalls are available to protect single computers. Check to see if your operating system's vendor includes this feature.

Review Accounts Regularly:
Everyone should regularly monitor their financial accounts for suspicious transfers and withdrawals. Businesses should monitor their accounts daily for suspicious transactions. Customers should notify Arundel Federal at 410-768-7800 immediately of any unexpected activity.

Change Your Passwords to Banking, Email, and Ecommerce Sites Regularly:
Passwords are the keys to your internet kingdom. Changing your passwords regularly will help ensure the security of all your online accounts as well as the information and the money they give you access to. When changing your password be sure to use strong passwords. Strong passwords use eight or more characters with random letters, numbers, and symbols. In addition, you should never use the same password on multiple sites. If one site is compromised your other accounts could possibly be accessed as well.

Be Careful What You Download:
You should never open email attachments or click on links in emails from people you don't know. You should also be wary of forwarded attachments and links from people you do know. Email attachments and links can circumvent even the best Antivirus software. . If you question whether a download is necessary to access a site you can always contact the company for further information.

Additionally, be wary of downloads from trusted and un-trusted sites that seem new or suspicious. If the site has been poisoned or compromised by hackers you could unknowingly be installing a virus or spyware. If you receive an email with a clickable link that requests that you contact a bank, insurance company, healthcare provider, etc., it is always best to close the email and type the URL of the web site directly in your browser rather than click the provided link

If Possible Have a PC Dedicated Only to Online Banking Activities:
Fraudsters and scam artists know that many individuals and small/medium sized businesses use online banking products. What they have also learned is individuals and businesses often do not take the time to adequately protect their PCs as outlined in these tips, nor do they regularly review their accounts for fraudulent activity. Using this knowledge fraudsters and scam artists are now actively targeting individuals and businesses using phishing attacks, email attachments, and web sites designed to take advantage of operating system and software flaws. One of the most effective controls is to use a second PC for your banking. This PC should not be used for regular web surfing, checking email, or other projects. These activities can increase your risk of unknowingly coming into contact with malicious sites and software. You should never use the computer your kids use for your online banking.