

• Welcome Message •

VantageSouth Bank handles a vast amount of sensitive information each day. Protecting this information is fundamental to our business. As a result, we have put into place a number of security measures that allow our customers to conduct business securely and with confidence. Technology alone, however, is not enough to thwart the attempts of mal-intended individuals. Security is as much a human issue as it is a technology issue.

While we can provide protections to prevent our services from being compromised, you must be responsible for protecting the security of your own information and PC. We hope this newsletter helps equip you with the security savvy necessary to protect yourself from the various types of fraud. If you find it helpful, feel free to pass it along to your friends, family and co-workers.

Future Newsletter Topics

-Published 3rd Monday of Each Month-

• **Issue 5:** What's The Difference Between ACH and Wire Transfer, Protecting Your Customer Data

• **Issue 6:** Protecting Your Business From Corporate Account Takeover, Understanding Your Hard Drive, Mobile Device Security

• **Issue 7:** Debit Card Safety, What To Do About Cyber Bullies, What Is A Cookie?

Creating Strong Passwords

We've taken strong measures to ensure the security and safety of our online banking system, but securing access to your accounts requires teamwork. You can help to keep your assets and computer systems secure by creating and maintaining strong passwords. Using strong passwords that are difficult or impossible to be discovered, and keeping them private, can keep strangers out of your accounts!

Weak passwords are cracked within minutes, giving cyber criminals access to online accounts. The more complex the password, the harder it is to crack. It's imperative that you take ownership of creating and using strong passwords that can act as a barrier between your private information and the thieves lurking about the Internet.

A strong password should:

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters, e.g. A-Z, a-z
- Have at least one numerical character, e.g. 0-9
- Have at least one special character, e.g. ~ ! @ # \$ % ^ & * () _ - + =

Examples of strong passwords:

- "Superman is super strong" *modified to* "Supermanis\$uperStrOng!"
- "Collect \$200 when passing go" *modified to* "C\$200wpG"
- "She loves you yeah, yeah, yeah!" *modified to* "sLuY3ah!"

By using strong passwords and keeping your computer free from malware, you can help us keep your online banking account safe and secure.

Is Your Business Being Protected?

We take our responsibility to our business customers very seriously, and while technology has provided a great convenience, it has also provided many risks. So, how do you protect your business from information compromise?

Here are a few tips to secure your online transactions:

- Offer ongoing training for your employees
- Use Multi-Factor Authentication to verify identities
- Install Firewall and Anti-virus programs
- Utilize intrusion detection and prevention systems
- Keep your operating system current
- Be vigilant about programs that you download
- Lock your computer whenever it is not in use
- Schedule an annual third party penetration test

Completing transactions online is not the only way information can be compromised. Make sure your employees understand that they need to secure their computer workstations as well. Passwords should be long and strong, and kept private. Ensure that employees do not keep passwords or security tokens in a place that could be accessed by people other than themselves.

Online Shopping Do's & Don'ts

DO your homework. Before entering your credit card information, take time to research the website and its policies.

DON'T buy from spammers. If you get an email inviting you to buy something like "Discounted Rolex's", you should think two things: 1) spam and 2) possible scam

DO consider contacting the seller if this is your first purchase. Most reputable e-sellers have a toll-free customer service phone number. This will assure you that a live person is available if needed post-sale.

DO buy from a website that has encryption. This feature automatically codes your personal data when it's entered. The URL should start with "HTTPS", "HTTP" or you should consider the site to be unsecure. Also locate the "Padlock" icon to verify a secure connection. Click on the "Padlock" icon to view more information about the site's security.

DON'T buy from a website with which you aren't totally comfortable. Just remember: "If it looks too good to be true, it probably is".

DO use computer security software. Keep your software updated by applying the latest service packs and patches. Refer to your operating system's help for assistance. This will reduce the risk of contracting a virus or some other form of malware.

DON'T forget to inspect your new purchase as soon as it arrives. If you find a problem, it's easier to fix it right away. Notify the seller as soon as possible.

DO check your credit card statements. Check your statements regularly so you know when something's gone awry.

Helpful Web Links

We encourage you to check out the following external resources:

- Federal Trade Commission: Consumer Protection
- FDIC: Consumer Protection
- USA.gov: Consumer Protection
- MySecurityAwareness.com