



Privacy and Security Newsletter

• 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 3:** Small Business Fraud Tips, Be Web Wise, Social Engineering
- **Issue 4:** Creating Strong Passwords, Is Your Business Protected, Online Shopping
- **Issue 5:** What's The Difference Between ACH and Wire Transfer, Protecting Your Customer Data

Phishing: Don't Get Hooked

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received an email with a similiar message? It's a scam called "phishing" - A phishing email can look just like it comes from a financial institution, e-commerce site, government agency or any other service or business. It involves hackers and cyber-criminals who are looking to lure personal information from unsuspecting victims. It often urges users to act quickly, to collect personal & financial information or infect your machine with malware and viruses.

How Do You Avoid Being a Victim?

- Don't email personal or financial information. Email is NOT a secure method of transmitting personal information. Before sending sensitive information over the Internet, check the security of the website (Look for https://).
- Pay attention to the website's URL. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.

Contact the company using information provided on an account statement, not information provided in an email.

- Keep a clean machine. Install and maintain anti-virus software, firewalls, and email filters to reduce spam.

What To Do If You Think You Are A Victim?

- Forward spam that is phishing for information to spam@uce.gov. Also alert the company being impersonated in the phishing email so they can be aware.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.
- File a report with the FBI's Internet Crime Complaint Center. (<http://www.ic3.gov>)

Spam, phishing and other scams aren't limited to just email. They're also prevalent on social networking sites. The same rules apply on social networks: When in doubt, throw it out. This rule applies to links in online ads, status updates, tweets and other posts.

Online Privacy: What Are You Sharing?

Every day, you give away personal information about yourself, sometimes without even realizing it. You do this when you take advantage of all kinds of services, including Internet searches, social networking, mobile and more. What private information are you sharing that you shouldn't? Use these tips to protect yourself:

1. Never give out your full name, address, birth date, or any other personally identifiable information that could be used to impersonate you or gain access to your accounts.
2. Read the privacy policies posted on websites and mobile apps before using their website, purchasing their product, or downloading their mobile app.
3. Update the privacy and security settings on your social networking sites to control who sees your posts and adjust them to your personal comfort level. Don't rely on the default settings. Be aware that both well-meaning and questionable people use social networks to gather information about you.
4. Don't post anything online that you wouldn't mind seeing on the front page of a newspaper.
5. Make sure that your password is long and complex. Don't reuse passwords on multiple accounts. Instead, choose unique passwords for each account, especially your online banking account.
6. Log out of websites and browsers when you're finished using them. Never leave your online accounts open.
7. Be wary of sites that offer a reward or prize in exchange for your contact information.

Top Cyber Security Threats

It's a dangerous world out there in cyberspace. Security threats are escalating every year and have become more malicious with cybercriminals stealing financial and personal information. Here's a quick look at some of today's top computer security threats:

1. **Malware.** Exploits and malware are increasing through vectors ranging from social networks to mobile devices to employees themselves. As computer and operating system security continues to improve so will cybercriminals' new techniques to bypass these defenses.
2. **Mobile Threats.** Attackers are turning their attention to launching mobile banking attacks. Keep in mind that if your smartphone becomes infected, it can infect your computer and your home or work network too.
3. **Threats to Mobile Payments.** Electronic currency has made sending money extremely easy. Buying or selling, and sending money from a mobile device is becoming more popular. Hackers know this and are increasingly targeting mobile devices to steal money.
4. **Attacks on SMBs.** Small businesses believe they are immune to cyber-attacks. Truth is, small companies are typically less equipped to defend against an attack and hackers take advantage of that.
5. **User Errors.** Computers are great. For many transactions, they are often better and more reliable than people. Humans make mistakes when using computers, especially when they're not savvy about computer security. Even if you think you're doing all you can to avoid common security threats, you'd probably be surprised at how easily an outsider can find, and take advantage of, common mistakes.

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](#)