# VantageSouth BANK

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

## Small Business Fraud Tips

Each year the Better Business Bureau is inundated with complaints from small businesses caught in fraudsters' webs. Perhaps it is an invoicing scam or being duped into paying for something they neither asked for nor wanted. There are costs to fraud that go far beyond and far deeper than the merely financial- the harm to a businesses' hard-won reputation chiefs among them. Knowledge and vigilance are keys to beating fraud. However, it never hurts to run down the list of well-known fraud types, so here they are:

- Directory Scams - A fraudster calls your business asking to update an entry in an online or printed business directory. The services are billed and paid for, but no listing is ever placed.
- Office Supply Scams - Fraudsters sometimes target small business owners by billing for office supplies that were never ordered hoping the business won't notice.
- Overpayment Scams - Be wary when a customer "mistakenly" overpays and then asks you to wire a refund. Later, when your financial institution goes to withdraw funds on the original payment, the frauster's account is empty. You do not get paid, and the refund you wired is gone.
- Data Breaches - An unauthorized leak of data, such as your customers' social security and credit card numbers, birthdates, addresses and more, can devastate the trust you have worked so hard to build.
- Vanity Awards- Beware of business "awards" in which you are required to pay for anything - trophies, plaques, and certificates. Many are just moneymaking schemes with no merit.
- Phishing E-mails - Phishing e-mails have been targeting small businesses to break into their computer networks. Fraudsters will claim to be the IRS pursuing an audit, or even the Better Business Bureau claiming to have received a complaint. Don't click on any links or attachments in a suspicious e-mail.

Knowing fraudsters' tactics and a few simple security tips - like those listed above - can help you and your small business beat fraudsters and stay fraud free.

# Be Web Wise

### Stay Current.
Keep pace with new ways to stay safe online: Check trusted websites for the latest information to share with friends, family and colleagues, and encourage them to be web wise.

### Think before you act.
Be wary of communications that implores you to act immediately, offer something that sounds too good to be true, or asks for personal information.

### Back it up.
Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

### Safer for me, more secure for all.
What you do online has the potential to affect everyone - at home, at work and around the world. Practicing good online habits benefits the global digital community.

## What is Social Engineering?

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

The goal of a social engineer is to fool someone into providing valuable information or access to that information. In most cases the attacker never comes face-to-face with the victim, but they get the information or the access they need to commit fraud nearly 100% of the time.

### Why are social engineers so successful?
Experienced social engineers relate well with others. They are consistently quick to establish a personal connection with the target and use that connection as the basis of building a rapport. The simplest way to get information is to ask for it directly, and this forms the basis for the various techniques used by hackers.

### Common social engineering techniques include:
1. Pretexting is when a social engineer developes a storyline that he or she is able to portray to the target. It provides the justification for the questions being asked.

2. Impersonation, such as posing as an employee, is arguably the best technique used by social engineers to deceive people because most people are basically helpful towards a coworker without question.

3. Phishing is a way of attempting to acquire information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

4. Dumpster Diving - Social Engineers commonly research a predetermined target and determine the best opportunities for exploitation. Dumpsters or trashcans with improperly discarded memos, bills and general mail, provide a huge amount of information that a hacker needs to impersonate an employee.

### How do you protect yourself?
The single most important key to avoiding social engineering attacks is to not give sensitive information to anyone unless you can verify that they are who they claim to be and that they have a legitimate need for access to the information.

## 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