Security Information

At Royal Business Bank, our first priority is protecting your identity and personal information. Learn what you can do to protect yourself against fraud and identity theft.

Identity theft is a federal crime in which someone wrongfully obtains and uses your personal information in a fraudulent or deceptive manner, usually for economic gain. It is reported to be the world's fastest growing crime. The most common ways thieves steal personal information online is through spoof emails, spoof websites, social engineering and other scams.

***IMPORTANT:** *Internet email is not secure. Unlike Online Banking, it does not use SSL encryption. Please do not send sensitive information, e.g., your social security numbers, account numbers, or other account information via email.*

Security Awareness

Educating yourself is the first line of defense against identity theft. Become familiar with and aware of any current issues or security threats that exist, by visiting the following sites:

http://www.fdic.gov/consumers/consumer/guard/
http://www.onguardonline.gov/
http://www.identitytheft.gov/
http://www.consumer.ftc.gov/articles/0076-phone-scams
https://www.ftccomplaintassistant.gov/Information#crnt&panel1-1

Email and Online Fraud

To protect yourself against email and online fraud, be very alert to unsolicited emails you receive from companies you conduct business with or know. The emails may contain clickable links for your convenience and the displayed text may be different than the actual link. Although fraudulent emails can be difficult to recognize, beware of emails that:

- **Request that you click a link** to a spoof website, one that looks like a real company website, including the real company's graphics and design. Since fraudulent email may even use exact wording from the real company's website, it's difficult to determine a spoof website. If you have any doubts, please contact Royal Business Bank at 888-616-8188 or send an email to cos@rbbusa.com (Central Operation Services). Unlike Online Banking, it does not use SSL encryption. Please do not send sensitive information, i.e. your social security numbers, account numbers, or other account information via email.

- **Ask you to give, confirm, or update sensitive personal information** such as Social Security numbers, usernames, passwords, PIN (Personal Identification Number) or account numbers.

- **Use Pop-Up windows** for entering or confirming personal data.

- **Have a sense of urgency** to give the information immediately, citing a specific thing that might happen. For example, your account may be closed or temporarily suspended.

- **Have spelling errors and/or bad grammar**. Intentional spelling errors may allow the email to get through spam filters used by ISPs (*Internet Service Providers*).

Learn ways to protect yourself as a consumer at www.ftc.gov/sentinel.
Visit www.fdic.gov and learn more about Phishing Scams.
Learn more about fraud prevention by visiting www.fakechecks.org.

Keep your Mobile Data Safe

Cellphones and tablets make life easier — unless they fall into the wrong hands.

You wouldn't leave your wallet lying around in a public place, right? Well, you should be just as diligent with your mobile devices. Follow these five essential practices to help protect you from becoming an identity theft statistic.

- **Use Passwords, Locks and More:** Always password-protect your mobile device, use the auto-lock security feature, and activate the encryption feature if one exists.

  Many devices can be set so that if the wrong password is entered a certain number of times in a row, the device automatically deletes all the stored information. But don't worry — you should be able to retrieve your data from your computer if you've been synchronizing the two devices.

  When creating a password, choose one that's easy for you to remember but will be difficult for others to guess. And make sure your auto-lock feature is turned on so it will kick in after a couple of minutes. That helps ensure no one will be able to use the phone or tablet without knowing your password. Also, don't share your password with anyone or tape it to your mobile device.

  While encryption offers some protection and may prevent unauthorized access to your mobile data, many mobile devices don't include this feature in their operating systems. Look in the owner's manual to see if your phone has encryption, and make sure the feature is included when you purchase a new phone.

  To encourage the return of a lost handset, consider writing or engraving your name and

contact information — but not your password — on its back with the promise of a reward. Several applications for cell phones let you offer a reward for the return of a lost phone.

- **Back It Up:** You should store only the information you think you'll need immediate and frequent access to in your mobile device. Remember, syncing your device to Outlook or another email application may automatically synchronize any notes in your contacts database, so pay special attention to what you have in those fields. Take care not to store user names and passwords in the note fields.

  Also make sure you have a separate record of the data, including all account numbers, passwords, phone numbers, addresses and any other sensitive information, as well as the device's make, model and serial number. Then, if your device is lost or stolen and you want to change your passwords quickly, you'll have the information you need at your fingertips.

- **Beware the Jailbreak and Out-of-Market Apps:** Such practices can open up your phone to substantial corruptions, such as viruses or Internet scams, without your knowledge. The only way to remove these harmful software threats, known as malware, is to completely wipe out the phone's memory and revert it to its original factory status.

  Just because your iPhone isn't jailbroken doesn't mean you're immune from risk. Apple says it rejects more than 100 spyware-infested or phishing-laden applications every day. The same risk applies to the Android. Beware of all apps downloaded from outside the Android Market. Out-of-market apps can be infected with viruses, Trojans and other malicious software applications that can steal your personal information. As hackers get more sophisticated with these devices, the possibility of malware increases. Mobile phishing apps — phony versions of real applications designed to separate you from your personal information — are also on the rise.

- **Pay Special Attention to Your Tablet:** Most tablets are thought of as overgrown cell phones that can be used for web browsing, video viewing and playing games. But tablets are just as capable as a phone — if not more so — of doing real work. They require the same amount of security foresight, yet few users even secure them with a password. Its larger size makes a tablet a more visible and natural target for would-be thieves. Because tablets are fully usable even without a cell phone plan, they are easier to resell on the black market.

  While a phoneless tablet may not contain your cellular directory, remember that it will have everything else: from web bookmarks to all your apps (complete with account information). Tablets have been touted for banking, investing and online shopping. You probably have a few apps along these lines installed, yet minimally secured. Letting your tablet fall into the wrong hands can be as disastrous as losing a phone.

- **Handle With Care:** If your mobile devices are lost or stolen:

- Call your provider to report the theft.
- File a police report (if you know it's been stolen).
- Place fraud alerts on your credit reports.
- Notify anyone whose contact or other information is stored in the phone.
- Consider using a remote wipe capability (if available) to prevent someone accessing your personal information. This feature gives you the ability to send a command to your device that will delete your data.

Protecting Your Business from Fraud

Businesses and consumers both need to be aware of the computer-related crimes affecting them. A guide, developed by the Federal Deposit Insurance Corporation (FDIC), provides cybersecurity information for business customers of financial institutions on how to safeguard their computer systems and data. The FDIC provides the following tips:

Protect computers and networks. Install security and antivirus software that protects against malware, or malicious software, which can access a computer system without the owner's consent for a variety of uses, including theft of information.

Patch software in a timely manner. Software vendors regularly provide patches or updates to their products to correct security flaws and improve functionality.

Require strong authentication. Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices, and online accounts by combinations of upper- and lower-case letters, numbers, and symbols that are hard to guess and changed regularly.

Control access to data and computers and create user accounts for each employee. Take measures to limit access or use of business computers to authorized individuals.

Teach employees the basics. Establish security practices and policies for employees, such as appropriate Internet usage guidelines, and set expectations and consequences for policy violations.

Train employees to be careful where and how they connect to the Internet. Employees and third parties should only connect to your network using a trusted and secure connection.

Train employees about the dangers of suspicious emails. Employees need to be suspicious of unsolicited e-mails asking them to click on a link, open an attachment, or provide account information.

Make backup copies of important systems and data. Regularly backup the data from computers used by your business.

Pay close attention to your bank accounts and watch for unauthorized withdrawals. Put in additional controls, such as mandatory confirmation calls before financial transfers are authorized with the financial institution.

Don't forget about tablets and smartphones. Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your business' network.

Watch out for fraudulent transactions and bills. Scams can range from payments with a worthless check or fake credit or debit card to fraudulent returns of merchandise.

Educate yourself. To learn more about protecting your business, visit the "Stop. Think. Connect." resources for small businesses at
http://www.dhs.gov/publication/stopthinkconnect-small-business-resources
and The U.S. House of Representatives Small Business Committee recently released cybersecurity guides for small business.

By following the information provided, learn how we fight fraud and identity theft, and what you can do to protect yourself.

If you have any questions or concerns about any unsolicited email that you receive, please contact Royal Business Bank at 888-616-8188 or send an email to cos@rbbusa.com (Central Operation Services).