

*As part of our concern for the protection of your personal information, Republic First Bank would like to share some information and tips to help you avoid becoming a victim of fraud and identity theft.*

## Phishing – What Is It and How to Avoid It

*"Creating a replica of an existing Web page to fool a user into submitting personal, financial, or password data"*

A phishing expedition is a two-pronged attack. First, the phisher creates a spoof email message: posing as a legitimate e-merchant operator or a financial institution, the phisher tries to lure a victim into visiting a web page. Once there, the phisher wants to lure you into completing a form or providing confidential information. The phisher hopes to gather as much of your personal, banking, credit, and other confidential data as possible.

### **The phisher is trying to steal your identity.**

This is how it works:

The first part of the e-mail or form appears legitimate enough by using brand colors and company logos. This is intentional, part of the overall strategy in tricking a user into revealing data. The phisher wants you to feel comfortable that this is really a legitimate communication from your bank or a merchant.

The phisher next asks for your credit card, checking, and bank routing information or other personal information. Some information requested should immediately set off alarms. The CVV (the 3 digit number printed on the back of the card) from a credit card is an anti-fraud security feature to help verify that you are in possession of your credit card. Use common sense here: if you enter the number in a web form, the phisher doesn't need to actually possess your card!

You should question any site that asks for your Social Security Number. As part of our security measures, Republic First Bank will **never** request that you enter your password, PIN or Social Security Number on a web form.

The final clue in this part of the phisher's attack is the request for your Credit/Debit card PIN. Again, use common sense: the Personal Identification Number is your "shared secret" with Republic First Bank. You punch it into an Automatic Teller Machine or brick-and-mortar store to withdraw money. You don't type it into a web form!

The final advice to avoid a phishing attack is to look at the address of the senders e-mail very carefully. This should show that it may appear to be originating from the bank or a respectable source but closer review will show you that there are some minor changes in the address and domain. This is a definite give away that this is an attempt to obtain your personal information. Should you not be sure if it is a legitimate correspondence, you may always call Customer Service to get confirmation at **1-888-875-BANK**.

## Identity Theft Protection

Identity-Theft is the fastest growing crime in America; 9.9 MILLION victims were reported last year, according to a Federal Trade Commission survey!

An identity thief takes your personal information and uses it without your knowledge. The thief may run up debts or even commit crimes in your name. The following tips can help you lower your risk of becoming a victim.

### **Here are the Top 10 Tips on Helping to Prevent Identity Theft:**

#### **✓Protect your Social Security number**

Don't carry your Social Security card in your wallet. If your health plan (other than Medicare) or another card uses your Social Security number, ask the company for a different number.

#### **✓Fight "phishing" – don't take the bait**

Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails and in the regular mail. Don't give out your personal information – unless you made the contact. Don't respond to a request to verify your account number or password. Legitimate companies do not request this kind of information in this way.

### ✓ **Keep your identity from getting trashed**

Shred or tear up papers with personal information before you throw them away. Shred credit card offers and “convenience checks” that you don’t use.

### ✓ **Control your personal financial information**

Most banks and other financial services companies will get your permission before sharing your personal financial information with outside companies. You also have the right to limit some sharing of your personal information with your companies’ affiliates.

### ✓ **Shield your computer from viruses and spies**

Protect your personal information on your home computer. Use strong passwords: with at least eight characters, including a combination of letters, numbers, and symbols, easy for you to remember, but difficult for others to guess. Use firewall, virus and spyware protection software that you update regularly. Always avoid the use of spyware. Download free software only from sites you know and trust. Don’t install software without knowing what it is. Set Internet Explorer browser security to at least “medium.” Don’t click on links in pop-up windows or in spam e-mail.

### ✓ **Click with caution**

When shopping online, check out a Web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, beware! Shop elsewhere.) Only enter personal information on secure Web pages with “https” in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers.

### ✓ **Check your bills and bank statements**

Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don’t arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.

### ✓ **Stop pre-approved credit offers**

Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).

### ✓ **Ask questions**

Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you’re concerned about identity theft. If you’re not satisfied with the answers, consider going somewhere else.

### ✓ **Check your credit reports – for free**

One of the best ways to protect yourself from identity theft is to monitor your credit history. You can get one free credit report every year from each of the three national credit bureaus: Equifax, Experian and TransUnion.

The following links can help provide more information on protecting you and your personal data:

<http://www.fdic.gov/consumers/privacy/criminalscover/avdthft.html>

<http://www.fdic.gov/consumers/consumer/idtheftstudy/>

<http://anon.vodium.com.edgesuite.net/anon.vodium/fdic/identitytheft/index.html>

<http://www.idtheft.gov/>

## **Document Management**

Another area that everyone should be aware of is proper document management and disposal. Too often people have found that discarded documents were responsible for stolen identities or credit card fraud.

An important step in protecting your personal information is to properly management sensitive documents. This includes items such as bank statements, credit card bills OR SOLICITATIONS and any document that may have your Social Security Number, Date of Birth, Driver License Number etc.

By simply throwing these documents into the trash, they now are vulnerable to being recovered and the information used to steal your credit and/or identity.

You should get into the habit of shredding these documents prior to disposing of them. Never discard intact documents containing confidential information. The important thing to remember is that by discarding these documents you make it easier for thieves to retrieve the information and use it against you. Some local communities host a “Shredding Day” at various locations where shredding machines are made available for your use. If one is nearby, take advantage of the opportunity. Simple precautions such as these can mean the difference between securing your personal information or becoming a victim.