

## Safer Online Banking

Online banking can be incredibly convenient and time saving. However, there is no absolutely safe online banking. But there are ways to make it safer. In this article you will learn about “phishing” schemes, how to avoid them, and general tips for safer online banking.

### What is "Phishing"?

**Phishing** is a general term for criminals creation and use of emails and websites, designed to look like emails and websites of well known legitimate businesses, financial institutions, and government agencies. These websites are used to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords.

The *phishers* then take that information and use it for criminal purposes, such as identity theft and fraud. A growing number of phishing schemes are using for illegal purposes the names and logos of legitimate financial institutions, businesses, and government agencies in North America, Europe, and the Asia Pacific region.

Ultimately, people who respond to phishing emails, and input the requested financial or personal information into emails, websites, or pop up windows, may be putting their accounts and financial status at risk in three significant ways.

- First, phishers can use the data to access existing accounts of those Internet users, and withdraw money or buy expensive merchandise or services.
- Second, phishers can use the data to open new bank or credit card accounts in the victims names, and use the new accounts to cash bogus checks or buy merchandise. If the phishers open those new accounts with the victims names, but use addresses other than the victims, the Internet users may not realize that they have become victims of identity theft until they are contacted by creditors or they check their credit reports.
- Third, some recent phishing schemes have involved the use of computer viruses and worms to disseminate the phishing emails to still more people.

### What Should Internet Users Do About Phishing Schemes?

The U.S. Department of Justice suggests three simple rules for Internet users when they see emails or websites that may be part of a phishing scheme: Stop, Look, and Call.

**1. Stop.** Phishers typically include upsetting or exciting (but false) statements in their emails with one purpose in mind. They want people to react immediately to that false information, by clicking on the link and inputting the requested data before they take time to think through what they are doing. Internet users, however, need to resist that impulse to click immediately. No matter how upsetting or exciting the statements in the email may be, there is always enough time to check out the information more closely.

**2. Look.** Internet users should look more closely at the claims made in the email, think about whether those claims make sense, and be highly suspicious if the email asks for numerous items of their personal information such as account numbers, usernames, or passwords. For example:

- If the email indicates that it comes from a bank or other financial institution where you have a bank or credit card account, but tells you that you have to enter your account information again, that makes no sense. Legitimate banks and financial institutions already have their customers account numbers in their records. Even if the email says a customer's account is being terminated, the real bank or financial institution will still have that customer's account number and identifying information.
- If the email says that you have won a prize or are entitled to receive some special *deal*, but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give you a real prize do not ask you for extensive amounts of personal and financial information before you are entitled to receive it.

Preventive Health Systems	Occupational Medicine Centers	<b>CONCERN<sup>®</sup> Services</b>	SHARE <sup>®</sup> Occupational Health Program	Work Capacity Services	TriHealth Fitness & Health Pavilion	TriHealth Executive Health Program
---------------------------	-------------------------------	-------------------------------------	--	------------------------	-------------------------------------	------------------------------------

**3. Call.** If the email or website purports to be from a legitimate company or financial institution, Internet users should call that company directly and ask whether the email or website is really from that company. To be sure that they are contacting the real company or institution where they have accounts, credit card accountholders can call the toll free customer numbers on the backs of their cards, and bank customers can call the telephone numbers on their bank statements. Do not call any numbers or click on any web links in the email as it is doubtful that they really lead to your financial institution or credit card company.

## For More Information

So what steps can you take to avoid being phished?

- Do not click on hyperlinks or respond to emails from your bank online. Go to its Web address on your own and check its messages for you at its site. Better yet, as suggested above, call.
- Before deciding to bank online, ask your bank how it is **authenticating** you or verifying your identity when you bank online. The best and newest technology not only verifies identity via personal questions, but it also can determine whether you are logging on from your own computer. If you are doing something out of the ordinary, your bank can follow with additional personal questions and/or a phone call.
- Keep antivirus, firewall and spyware protection up to date and on.
- Never use your debit card online. Most credit card companies and banks have policies that will protect you against fraudulent use of your credit card online or otherwise. However, by the time a crook gets caught with your debit card number, your checking and possibly savings account could be wiped out. Even if your bank has a policy that protects you, it may take weeks to get that money back.