The Cooperative Bank (TCB)
Online Banking Tips to keep you safe!

Online banking is a handy way to keep track of your personal and business finances. You simply log on through TCB's website, and you can do things like check your balances, pay bills, transfer money between appropriate accounts, and order checks.

For convenience sake, you can't beat an online bank!

However, the popularity of online banking has not gone unnoticed by the cyber criminals. According to Shawn Henry, Executive Assistant Director of the FBI, “Some of the most critical threats facing our nation today emanate from the cyber realm. We’ve got hackers out to take our personal information and money, spies who want to steal our nation’s secrets and terrorists who are looking for novel ways to attack our critical infrastructure.”

At TCB we want to help you, our customers, understand the types of popular attacks on your money, and what you can do to prevent them.

Phishing

One of the most common ways that a criminal will attempt to part you of your money is through something known as Phishing. Phishing is pronounced FISH-ING. It's the Internet's equivalent of this popular sport. The fisherman is a criminal, the bait is usually an email that attempts to panic you into action, and the fish is you!

The criminal sends out thousands of email using a list he got from a spammer. The email sent pretends to be from a bank. Let's call it “My Bank”. Most of the recipients of the email will not have an account with My Bank. But some will. It's those few account holders that the criminal is after.

In the email, you may be warned that you need to update your personal banking information, and that it's essential that you act **now** to protect your account. They'll usually try to scare you into taking action and there's always a link for you to click. When you click on the link, you’ll be taken to an un-secure area where you will be prompted to enter your personal information.

This page will look like the bank's website. **Except it's not!** One trick the criminal may use is to have an address that looks similar to that of your bank. For example, your real bank’s website may be: https:\\www.mybank.com.

If you take a closer look at the address bar from the phishing email, you may see something like this: http:\\www.mmybank.com

The address has been spoofed. An extra “m” was added to the address. But some spoofed addresses are more difficult to spot and even fool the more experienced surfers. Be sure to look for other clues in your browser!

🔒One thing that all browsers will have is a padlock icon. These icons are used to indicate that the website is using security measures. Click on the padlock and you'll see information about the security certificate. Check your browser version for the appropriate security lock icons. Understand them for security sake.

One more thing to note: The address for a secure site normally starts with https. If the "s" is missing, it's not a secure site!

A last word of warning, these visual clues have been known to be spoofed by the criminals! So if in doubt, remember this:

TCB will <u>NEVER</u> send you an email asking for your login details!

If you receive such an email, contact us and we will instruct you on how to handle the message. And remember, DON'T click on the link!

The same is true for other secure websites that hold your money. They never send you emails asking you to confirm your personal information! For a more detailed look at Phishing, there's an excellent Wikipedia article. Go to the site and search “phishing.”

The latest versions of Firefox and Internet Explorer have anti-Phishing measures built in. You should make sure these are turned on when accessing secure websites.

Password Protection

We've all got passwords. In fact we've all got LOTS of passwords! We've got so many that it's become increasingly difficult to keep track of them all. Banking passwords are no different. But the recommendation is to keep changing each one every few months or so! Yes it’s a pain but worth the security.

Because the password process can be cumbersome, some people have one password for all of the sites on the internet that ask for them. **<u>This is something you should NEVER do</u>**! You need a different password for each site. The reason is simple - if a criminal has your password for one website, he's got them ALL - he could clean you out!

How do you remember them all? It’s a challenge, but be safe and creative. Here are a few suggestions:

- Use words from your favorite song
- Replace a letter for a number for example E =3, O=0
- Mix it up– use upper and lower case letters, numbers and if able special characters.
- Always capitalize certain letter such as all the A or C’s

Also, remember that short passwords are easy to crack. Always use at least 8 characters. And **do NOT share passwords! If you share, YOU are responsible for the security breach.** If you use Business Banking and a staff member leaves, remember to change the password immediately so his/her access to your data is disabled.

You and Your PC

You should never log in to your bank account using somebody else's computer. Simply because you have no idea what security measures are in place and whether or not the computer is infected.

Internet cafes are also not where you should be entering secure information. In an internet cafe, all the data you enter is logged and saved by the owners (they may be forced to do this by law). You can never be sure that your data is safe from prying eyes. Also, what if you forget to log out properly? The next person who uses the computer could see all of your personal information and have access to your bank account!

The only place you should be entering your bank information is your own PC. Of course, you need to make sure that your own computer is safe from infection, and take sensible security measures when it comes to the emails you receive. Follow the suggestions below and your PC will be much more secure than it was yesterday!

- If the financial risk is high use a separate PC for online banking. Make sure you still follow all the protection tips as well.
- Protect your workstation with an updated antivirus and malware program. You should subscribe to your antivirus software's updating service which will keep your software updated with the latest virus tools.
- Set your PC to automatically perform the update from your antivirus software. If you chose to set up a manual system, keep track of when you do it and check it daily.
- Keep your operating system (OS) and programs up to date by subscribing and installing the latest patches.
- Use only Microsoft and Apple supported operating systems.
- For Business customers a cellphone or landline may be needed to verify your login to online banking. If this option is available it is a recommended selection.
- Currently supported browsers for online banking are as follows: Microsoft Internet Explorer (IE), Google Chrome, Safari and Firefox. TCB only supports the latest two versions of the browser.
- A minimum of 128 bit SSL encryption will be needed to connect to the online banking portal.

Again, for convenience sake you can't beat an online bank! And always remember the safety tips to help keep you safe.