CIBM BANK

CENTRAL ILLINOIS BANK
MARINE BANK
Milwaukee | Indianapolis
AVENUE BANK
A branch of CIBM Bank

Protect Yourself From Online Banking Fraud

CIBM Bank is committed to protecting your personal and account information. We have account monitoring systems and other controls in place to recognize and help prevent fraud.

CIBM Bank will never attempt to gain your personal or account information via email, text message or automated phone calls. Attempts such as these should be considered fraud. If you are contacted in this manner or believe you are the victim of bank fraud, contact your local branch immediately for assistance.

The online banking industry has seen an increase in fraudulent activity over the last several months. With keystroke loggers, virus attacks and phishing scams becoming more prevalent, are you doing all you can to protect yourself from becoming a victim of fraud?

Many cyber criminals don't want to steal your identity in the traditional sense, they simply want to take your money and move on to the next victim. While most companies that do business on the Internet including Financial Institutions are very diligent in providing online protection for their customers, the first line of defense is knowledge about what you, the end-user, can do to protect yourself.

- Use Anti-Virus Software and make sure that it stays up-to-date. This is the single most important thing you can do to protect your computer from viruses.
- Keep your Operating System up-to-date with the latest security patches.
- Never click on a link from a business requesting that you provide them with personal information.
- Pay close attention to the URL (Internet address) behind the link. Often in phishing attempts, if you hover the cursor over the link the fraudsters want you to click on, it has nothing to do with the actual company they claim to be. Report any phishing attempts to your Financial Institution.
- If your Financial Institution uses watermarks or personal images, do not log in unless you see the correct image on the screen.
- Change your passwords often. Even if your financial institution doesn't require it, it is a good practice to change your passwords at least every six months.
- Don't use the same ID and PIN/Password for every online account you have.
- Never disclose your login credentials to other people or companies.
- Do not store your ID and Password information where others could gain access to it. It is best not to write the information down at all.
- Do business with a financial institution that offers two-factor authentication for accessing your information online. If offered by your financial institution, take advantage of hard- or soft-tokens, which provide a unique one-time-use password each time you access your account. This is especially important for business accounts with multiple users.
- If accessing information via a wireless network, ensure that the network is secure. Accessing sensitive information (or any website) over a non-secure network simply leaves the door open for criminals.
- Experts recommend and caution that banking transactions should be executed on a PC used only for that purpose and not exposed to the broader internet through surfing and other activities.