



SECURITY

At First Commercial Bank (USA), we are fully committed to protect your information. We understand your information is valuable and we take measures to safeguard it the moment you login to our website or mobile application.

Secure Authentication

From the moment you login to our website, your authentication information is protected via advanced encryption technology, which prevents unauthorized people from intercepting your credentials.

You can validate the encryption technology on your website by ensuring the link starts with https (not http).

Multi-Factor Authentication (MFA)

For certain types of sensitive activities, we require you to use MFA as an additional layer of protection. MFA is designed to prevent instances where stolen username and password are misused.

It is important to verify that only authorized persons log into online banking. This is achieved by verifying your password. When you submit your password, it is compared with the password we have stored in our secure data center.

We allow you to enter your password incorrectly a limited number of times; too many incorrect passwords will result in the locking of your online banking account until you call us to reinitialize the account. We monitor and record "bad-login" attempts to detect any suspicious activity (i.e. someone trying to guess your password).

Electronic Funds Transfer Act. Please refer to your Electronic Funds Transfer Act Disclosure for details.

Session Timeout

To reduce the risk of unauthorized people from seeing your private account information, we enabled automatic timeout of your browser session. This happens when we detect your session to be idle for a period of time.

Behind the Scenes

First Commercial Bank (USA) uses a combination of security technologies behind the scenes to safeguard your information. We understand the cyber world is constantly changing and



therefore we continuously update our technology to maintain a secure environment. We also periodically test our security controls to validate their effectiveness.

Ways to Protect Yourself

Spotting Phishing Scams

Phishing is a technique used to trick you into divulging sensitive information such as your online password or account number. Phishing comes in the forms of emails, voicemails, text messages and even traditional mail.

While phishing campaigns are getting more sophisticated, most of them still leverage common methods, including:

- Asking you to click on a link, open an email attachment, or call a number
- Asking you to divulge your private information
- They often contain spelling errors
- Using scare tactics or authoritative tone

What You Can Do

Keep in mind that First Commercial Bank (USA) will never ask you to reveal your password.

- Do not respond to messages that ask you to reveal your sensitive information
- If you receive a message from someone you know and it looks suspicious, then contact that person directly to verify the message
- Update your computing systems with the latest operating system version; this applies to PC, Mac and mobile devices
- Install a reputable anti-malware solution and keep it updated as well
- Enable pop up blockers on browsers

You play a crucial role in preventing others from logging on to your account. Never use easy-to-guess passwords. Examples:

- Birth dates
- First names
- Pet names
- Addresses
- Phone numbers
- Social Security numbers

Never reveal your password to another person. Do not write your password down. You should periodically change your password in the User Option screen of online banking.

Use a different password to access your online banking accounts than the ones you use for other applications.



Always log off your online banking session before leaving your computer.

We will NEVER email you for your personal information. Any email claiming to be the bank requesting personal information such as Social Security numbers, IDs, or passwords should not be trusted.

Contact Us with Questions

- For more information, please contact us [here](#).