UNDERSTANDING
RANSOMWARE

RANSOMWARE prevents access to important files.

Ransomware, known as "malware", is a type of malicious software designed to hold data hostage. This malware encrypts, or conceals access to the victim's files in attempt to get them to pay a ransom to regain access. This is a growing threat for both individuals and businesses alike.

Risks of Ransomware

- Ransomware costs businesses more than $75 billion a year.
- Temporary or permanent loss of sensitive information.
- Financial losses to restore systems and files.

The most common targets for ransomware attacks are small to medium-sized businesses, school districts, municipalities, health-care institutions and financial institutions.

What can you do?

Use a reputable anti-virus software, email filtering and a firewall. Limit internet connectivity and define user accessibility. Employ proper network segmentation.

Attachments may be malware or spying software. Files with .exe, .scr, .zip or .bat endings are red flags. Call companies directly, using a phone directory - not the number in email, to verify attachment.

STOP. **THINK. DON'T BE FOOLED.**

Notify your bank immediately if you have given out your information, so they can help protect your account.

RCBBank.com/Security
Fraud Dept. 877.361.0814

RCB BANK