

## Preventing Business Fraud

Keeping your business' sensitive information secure is critical. Here are some ways you can prevent fraud in your company:

- Password-protect laptops and encrypt sensitive files.
- Install, use and regularly update anti-virus and anti-spyware software on your computer or network.
- Use a firewall to prevent hackers from invading your computer/network.



- Educate employees not to respond to or click links within suspicious e-mails as they can potentially infect their computers with keyloggers or other malicious software.
- Protect statements that contain account numbers.
- Run background checks on applicants prior to granting access to sensitive information or purchasing authorization.
- Segregate duties so no employee is responsible for both recording and processing a transaction.



Bank of Commerce will never request your personal information via an unsolicited email or phone call. We will never call you requesting your card number, PIN, expiration date, or 3-digit number. Please report any suspicious requests to: [idtheftinfo@reddingbankofcommerce.com](mailto:idtheftinfo@reddingbankofcommerce.com)



## Fraudulent ACH Transfers Connected to Malware:

Within the last several months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts.

In a typical scenario, the targeted entity receives a "spear phishing" e-mail which either contains an infected attachment, or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware is installed on their computer.

The malware contains a key logger which will harvest each recipient's business or corporate bank account login information. Shortly thereafter, the perpetrator either creates another user account with the stolen login information or directly initiates funds transfers by masquerading as the legitimate user. These transfers have occurred as both traditional wire transfers and as ACH transfers.

Visit [the Internet Crime Complaint Center](#) for more information.



## Four Rules to a Great Password

**#1.** A good password is **at least** eight characters long.

**#2.** Use a mix of **at least** three of these four things: small letters (a, b, c), capital letters (A, B, C), numbers (1, 2, 3), and symbols (!, @, #).

**#3.** Don't use easy-to-guess passwords.  
example: names, cars, home address, employer, favorite singer, dictionary words, (even if they're words from other languages) and so on.

**#4.** Good passwords are easy to remember and hard to guess.  
example: Easy to remember, Easy to guess: "password", "QWERTY", "123456"

So how do we come up with a good password that has at least eight characters in it, uses a mix of small and capital letters, numbers, and symbols, isn't easy-to-guess, and is easy to remember?

[Here's how.](#)