# BUSINESS CUSTOMERS

## Protect Yourself from Fraud & CATO

The most common way fraudsters attack small businesses is by Corporate Account Takeover (CATO) – when cyber thieves gain control of a business's bank account by stealing the business's valid online banking credentials. Although there are several ways this can happen, the most prevalent involves malware that infects a business' computers. Cyber thieves use online banking sessions to initiate funds transfers, by ACH, wire transfer or other electronic banking products.

Small businesses are targeted because they don't often have the same level of security features that larger businesses may have in place to keep their information secure. Many small businesses do not monitor and reconcile their accounts on a frequent basis.

Preventing fraud is a joint effort between the financial institution and the customer. Listed below are things that you are responsible for doing and things that we do for you.

## YOUR *Responsibilities to Prevent Fraud*

### Passwords

- Create strong passwords.
- Change passwords frequently.
- Prohibit the use of "shared" usernames and passwords.
- Never share username and passwords with third-party providers.

### Online Banking

- Access online banking activities from a stand-alone computer system from which email and web browsing are not possible.
- Verify use of a secure session ("https") in the browser.
- Never access bank information at Internet cafes, public libraries, etc.
- Never leave a computer unattended while using online banking.
- Only give access to people who are authorized on your account. You are responsible for their actions.

### Email

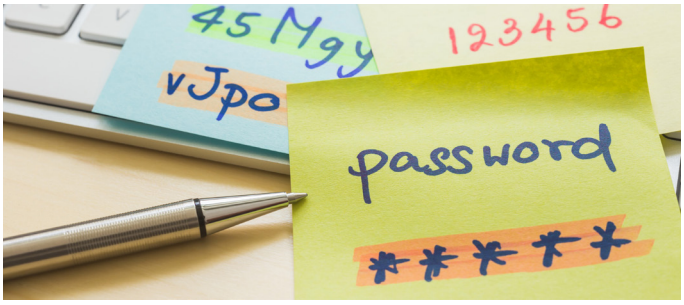
- Be suspicious of emails purporting to be from a financial institution, government or other agency requesting account information or verification of usernames, passwords, PIN codes, etc. If you are not certain of the source, do not click any links.

### ACH & Wire Transfers

- Initiate ACH and wire transfers under dual control, with a transaction originator and a separate transaction authorizer.
- If you get an email or ACH change request, make a phone call to verify the request.

### Other

- Reconcile all transactions on a daily basis watching for unauthorized or suspicious activities.
- Regularly review user access levels, dollar limits and activity.
- Install computer security tools such as firewalls, anti-virus software, and spyware detection programs and remember to update regularly.
- Regularly update your financial institution with your current contact information.
- Immediately report any suspicious transactions to the financial institution.
- Respond promptly to inquiries from the bank.



# Protect Yourself from Fraud

## United Bank of Iowa Provides for YOU

**Secure online platform** with options so you can set up alerts to assist you with monitoring your account.

**Multi-Factor Authentication** (MFA) as an additional method of authenticating an online banking user, including these features:

- Monitors login/device
- Monitors transactions
- Online security feature – detects uncharacteristic or unusual behavior involving your account. If anything out of the ordinary is detected, we will verify your identity by asking you to verify your passcode or password to make sure it's really you.

**Transaction limits** set within the system for bill pay and bank to bank transfers to minimize risk.

**Security recommendations and guidelines** to accountholders.

## What to Do if You Suspect Fraud

- Immediately cease all activity from your computer system. (Disconnect your network connections to isolate the system from remote access.)
- Immediately contact your bank for assistance with the following: reviewing recent transactions and electronic authorizations, disabling online access to accounts, changing online banking passwords and opening new account(s) when appropriate.
- Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents to be sent to another address.
- Maintain a written chronology of what happened, what was lost and the steps taken to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.
- File a police report and provide the facts and circumstances surrounding the loss. Having a police report on file may be helpful when dealing with insurance companies, banks and other establishments. The police report may initiate an investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.