Business Security Center

A critical aspect of better money management is protecting it. The privacy and security of your business and account information is extremely important to us. Using some basic security practices, we can work together to fight fraud and help ensure the protection of your company's private information. Please browse the information below to learn more.

Corporate Account Takeover

Corporate Account takeover is the business equivalent of personal identity theft. Hackers, backed by professional criminal organizations, are targeting small and medium businesses to obtain access to their web banking credentials or remote control of their computers. These hackers will then drain the deposit and credit lines of the compromised bank accounts, funneling the funds through "mules" that quickly redirect the monies overseas into hackers' accounts.

As a business owner, you need an understanding of how to take proactive steps and avoid, or at least minimize, most threats.

- Use a dedicated computer for financial transactional activity. DO NOT use this computer for general web browsing and email
- Apply operating system and application updates (patches) regularly
- Ensure that anti-virus/spyware software is installed, functional and is updated with the most current version
- Have host-based firewall software installed on computers
- Use latest version of internet browsers, such as Explorer, Firefox or Google Chrome with "pop-up" blockers and keep patches up to date
- Turn off your computer when not in use
- Review your banking transactions and your credit report regularly
- Contact your Information Technology provider to determine the best way to safeguard the security of your computers and networks

Call us immediately at (207)786-5700 if you believe that your Mechanics Savings Bank account has been compromised.

Social Engineering

Social Engineering is a technique used to obtain or attempt to obtain secure information by tracking an individual into revealing the information.

Social Engineering is normally quite successful, because most targets (or victims) want to trust people and provide as much help as possible.

Victims of Social Engineering typically have no idea they have been conned out of useful information or have been tricked into performing a particular task.

The easiest way to breach security is to obtain credentials and the easiest way to get that information is to ask someone for it.

The basic goal of Social Engineering is to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply disrupt and compromise computer systems.

Common Techniques

- Social Engineering by phone — Pretexting
- Dumpster Diving
- Online Social Engineering — Phishing, Vishing, SmiShing, Pharming
- Persuasion
- Reverse Social Engineering
- And many more…

What you should do

- Never share your user name or password with anyone
- Mechanics Savings Bank will never call for your user name or password
- ALWAYS be aware of your surroundings

Mechanics Savings Bank will never request customers' personal information by phone, through email or provide links within an email to update information. Beware of Vishing Attempts. Vishing is an attempt to obtain personal information, card information or account information under false pretenses through the use of a telephone. Please note that this is not from us. If you do receive a phone call like this, please call our customer Service Center at 207-786-5700 with any information you may have.

E-Mail Scams

Protect yourself from internet and email scams by keeping your private information secure. Mechanics Savings Bank will never request customers' personal information by phone, through email or provide links within an email to update information.

Here are a few ways you can protect yourself from Internet and E-Mail fraud:

- Never click on links in unexpected e-mails that request confidential information.
- Before submitting confidential information through forms, make sure you are using a secure internet connection.

- Make sure you have installed and run updates anti-virus and anti-spyware software. Anti-virus and anti-spyware software will keep your computer safe from malicious software that might have installed itself on your computer.
- Install a firewall, either software or hardware. A firewall is especially important if you are using a broadband internet connection like DSL, cable, or satellite.

MEAPC (Maine Anti-Phishing Coalition). 21 Banks located throughout the state of Maine have joined together to form the Maine Anti-Phishing Coalition (MEAPC). The MEAPC Banks embrace a mission of preventing information theft & fraud through public education and awareness

OnGuard. OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Mechanics Savings Bank utilizes the following Security Procedures in connection with its Business Online Banking Services:

We provide our Customers with multifactor authentication through the use of User ID's, passwords and a One-Time access code sent via phone, text or email to access the Services.

Mechanics Savings Bank has deployed Enhanced Login Security which is a new online security feature that provides additional protection from fraud and identity theft. By recognizing your login identification and your computer, Enhanced Login Security verifies that you are authorized to have access to the online system. To learn more about what this means when you login please go to http://www.mechanicssavings.com/home/brochure and down load Business Online Banking Enhanced Login instructions.

We also provide Customers with a User Guide and access to online help screens within the application.

We prompt Customer to reset Customer passwords every 90 days.

We provide a layered approach to security for all high risk Online Banking Services, such as ACH Payment Services and Wire Transfer Services which includes;

a. The use of dual customer authorization through different access devices (e.g. passwords, one-time access codes, and tokens)
b. Enhanced control over account activities by establishing transaction value thresholds.
c. Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels.
d. Require dual control and approval before the transaction is initiated.

e. Enhanced customer education to increase awareness of the fraud risk and effective techniques that customer can use to mitigate this risk through; annual customer education seminars; website updates; direct email communication.

Mechanics Savings Bank recommends that Customers implement and utilize the following Security Procedures in connection with use of the Services:

Segregate duties when originating ACH and or Wire transfers.

Use of the voice option for one-time access code over text or email.

Un-enroll a computer by removing the cookie from the computer so it is no longer recognized for authentication.

Use a dedicated computer for online banking purposes that is never used for e-mail or general internet browsing/surfing.

Review pending payment and transfer instructions prior to their submission to the Bank to ensure that they are complete, accurate and properly authorized.

If Customer notices suspicious account activity or believes the security or confidentiality has been or may be breached, you may contact us at one of the following Mechanics Savings Bank numbers:

- **Deposit Operations Department; (207) 786-5700 ext. 4179**
- **Security Officer; (207) 333-4577**
- **Relationship Officer (207) 786-5700**