












Protect your business against Fraud

At Monarch/OBX Bank, the security of your confidential information and your assets is a top priority. With more of our financial activities occurring over the Internet, it is important to be aware of risks associated with these services and steps you can take to reduce the risk that someone will illegally gain access to your private information or financial accounts.

The most important thing to remember is that Monarch/OBX Bank will NEVER request personal information (ex. your social security number, account number, PIN, user ID or password) through email or unsolicited phone calls.

We strongly recommend that commercial clients exercise caution to help prevent fraud.

Following are some suggestions:

-  **Never write down your passwords.**
-  **Unique IDs:** Make sure that everyone needing online access has their own User ID and Passwords. Sharing login information should be prohibited. Never share usernames, passwords, PIN codes or similar information.
-  **Dual Control:** Implement a system of dual control and approval for ACH and wire transfers where dual approval is required prior to the transaction being initiated.
-  **Strong Passwords:** Use the maximum characters allowed, and be sure to include a combination of mixed case letters, numbers and special characters (when permitted).
-  **Random Passwords:** Avoid using personal information like family or pets' names, or your date of birth.
-  **Unique:** Use separate passwords for work related and non-work related accounts. Do not use the same password for all of your online accounts.
-  **Private:** Remind your staff to NEVER share login information with third-party providers.
-  **“Do not remember me”:** Encourage your staff NOT to take advantage of automatic login features. It is best to type in your User ID and Password each time you login, instead of using systems that pre-populate the login fields.
-  **Administrators:** Limit administrative rights on users' workstations. This will help prevent the inadvertent downloading of malware or other viruses.

In the event you notice suspicious account activity or have fraud related to your account, please call 757-389-5152 option 1 or your local Monarch/OBX Bank branch immediately.









Protect your business against Fraud

At Monarch/OBX Bank, the security of your confidential information and your assets is a top priority. With more of our financial activities occurring over the Internet, it is important to be aware of risks associated with these services and steps you can take to reduce the risk that someone will illegally gain access to your private information or financial accounts.

The most important thing to remember is that Monarch/OBX Bank will NEVER request personal information (ex. your social security number, account number, PIN, user ID or password) through email or unsolicited phone calls.

We strongly recommend that commercial clients exercise caution to help prevent fraud.

Following are some suggestions:

-  **Virus Protection:** Install commercial grade anti-virus, anti-malware and desktop firewall software on all computer systems, and be sure to update the software regularly. An actively managed firewall helps to limit the potential for unauthorized access to a network and computers.
-  **Stay Current:** Computers should be patched regularly. It is particularly important to apply security patches to operating systems and key applications, both of which should have automatic updates to prompt you to patch the system.
-  **Physical Access:** Control physical access to your computers and network components. Prevent access or use of business computers by unauthorized individuals. Laptops should be stored securely when unattended.
-  **Avoid Public Computers:** Never access Online Banking, or any other financial services from a public computer at a hotel/motel, library or public wireless access point. Unauthorized software may have been installed on these public machines, and could be trapping account information without your knowledge.
-  **Email attachments:** Opening attachments or clicking on links embedded in suspicious emails could expose your system to malware. Be cautious when opening emails, especially when they appear to be from a financial institution, government department or other agency.
-  **Power Employees:** Change, revise, and re-visit those IT employees who have “keys to the kingdom” access for user approval, access rights, and deleting/adding new users. While many attacks occur from outside hacking, insider hacking does occur, and dividing or rotating “keys to the kingdom” IT authority can cut down on opportunities for insider fraud.

In the event you notice suspicious account activity or have fraud related to your account, please call 757-389-5152 option 1 or your local Monarch/OBX Bank branch immediately.



Protect your business against Fraud

At Monarch/OBX Bank, the security of your confidential information and your assets is a top priority. With more of our financial activities occurring over the Internet, it is important to be aware of risks associated with these services and steps you can take to reduce the risk that someone will illegally gain access to your private information or financial accounts.

The most important thing to remember is that Monarch/OBX Bank will NEVER request personal information (ex. your social security number, account number, PIN, user ID or password) through email or unsolicited phone calls.

We strongly recommend that commercial clients exercise caution to help prevent fraud.

Following are some suggestions:

- 🦋 **Computer Cache:** Clear the browser cache before and after an Online Banking session. This helps eliminate copies of web pages that have been stored on the hard drive.
- 🦋 **Education:** Ensure all personnel understand the importance of good cyber security practices. In particular, make sure that your employees with account access know the best practices for Online Banking.
- 🦋 **Monitor activity:** Routinely check and reconcile bank accounts, credit and debit card statements to ensure that all transactions are legitimate – preferably on a daily basis.
- 🦋 **Stay Alert:** When banking or shopping, look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "http://" is not secure.
- 🦋 **Stay in Session:** Never leave a computer unattended while using Online Business Banking or financial services. For most systems, timeout features can be adjusted to an appropriate setting to prevent unauthorized access online.
- 🦋 **Limit Web surfing:** Limit or eliminate unnecessary web-surfing and/or email activity, including personal activity, on computers used for online banking. Many hacking attacks use social networking sites (such as Facebook) to transmit computer viruses.
- 🦋 **Green Address Bar:** A green address bar indicates that the website has been secured with Extended Validation (EV) SSL by [VeriSign](#). Monarch/OBX Bank passed a rigorous identification process conducted by VeriSign, the most recognized SSL provider on the Internet.

In the event you notice suspicious account activity or have fraud related to your account, please call 757-389-5152 option 1 or your local Monarch/OBX Bank branch immediately.



Protect against Fraud

At Monarch/OBX Bank, the security of your confidential information and your assets is a top priority. With more of our financial activities occurring over the Internet, it is important to be aware of risks associated with these services and steps you can take to reduce the risk that someone will illegally gain access to your private information or financial accounts.

The most important thing to remember is that Monarch/OBX Bank will NEVER request personal information (ex. your social security number, account number, PIN, user ID or password) through email or unsolicited phone calls.

Other information

- 🦋 www.StaySafeOnline.org - Website of the National Cyber Security Alliance, sponsored by the Department of Homeland Security and the Federal Trade Commission.
- 🦋 www.ftc.gov/idtheft - The FTC's Website for information about Identity Theft.
- 🦋 Learn how to disable the geotagging feature on your phone at <http://icanstalku.com/how.php#disable>.
- 🦋 You have the right to ask that nationwide consumer credit reporting companies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer credit reporting companies. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.
 - 🦋 Equifax: 1-877-576-5734; www.alerts.equifax.com
 - 🦋 Experian: 1-888-397-3742; www.experian.com/fraud
 - 🦋 TransUnion: 1-800-680-7289; www.transunion.com
- 🦋 An initial fraud alert stays in your file for at least 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a consumer credit reporting company will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency.

In the event you notice suspicious account activity or have fraud related to your account, please call 757-389-5152 option 1 or your local Monarch/OBX Bank branch immediately.