












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.

Avoid becoming a victim of phishing and other scams

-  **Caution:** Be suspiciously cautious of any immediate requests for personal financial information via email.
-  **Proactive Protection:** Ensure that your computer has appropriate spam filtering, anti-virus and anti-spyware and firewall software. Also ensure all software is current and up to date.
-  **Email links:** Do not click on links within emails that ask for your personal information.
-  **Email attachments:** be cautious of emails with attachments from unknown or unreliable sources. Generally, do not open any emails unless you are expecting it or know the source.
-  **Personal information:** Never enter your personal information in a pop-up screen. Only communicate personal information via a trusted source such as a secure Website.
-  **Beware of "pharming":** Beware of virus or malicious programs secretly installed in your computer to hijack your Web browser. These viruses take the user to a fake copy of a website without the user realizing it. Any personal information you provide at the phony site, such as your password or account number, can be stolen and fraudulently used.
-  **Beware of "phishing":** Hackers use this technique to steal personal information (such as passwords) to commit fraud. Phishing can be done over the internet, text messaging or by phone.
-  **Monitor activity:** Routinely check and reconcile bank accounts, credit and debit card statements to ensure that all transactions are legitimate.
-  **Computer Security:** Ensure that your web browser is up to date and security patches applied.

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.

Ensure safety and security online

- 🦋 **Never write down your passwords.**
- 🦋 **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.
- 🦋 **Strong Password:** The greater the variety of characters in your password the better, so be sure to make your password alphanumeric, and, if permitted, use special characters.
- 🦋 **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.
- 🦋 **Beware:** If you ever feel that your information has been compromised, change your passwords right away.
- 🦋 **Secrecy:** Do not share your passwords with anyone. They are for your knowledge only.
- 🦋 **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.
- 🦋 www.StaySafeOnline.org - Website of the National Cyber Security Alliance, sponsored by the Department of Homeland Security and the Federal Trade Commission.

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.

Mobile devices

-  **Keep security software current:** Having the latest revision of mobile security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Security protections are updated on a regular basis. This may require synching your device with a computer.
-  **All Around Security:** Protect all devices that connect to the Internet. Computers, smart phones, gaming systems, and other web-enabled devices need protection from viruses and malware.
-  **Secure your phone:** Use a strong passcode to lock your phone.
-  **Think before you app:** Review the privacy policy and understanding what data (location, access to your social networks) on your device an app can access before you download it.
-  **Protect your number:** Only give your mobile number out to people you know and trust and never give anyone else's number out without their permission.
-  **Wi-Fi care:** Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.
-  **When in doubt, don't respond:** Fraudulent texting, calling and voicemails are on the rise. Just like email, requests for personal information or immediate action are almost always a scam.

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://www.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.