



Report Phishing and Email Scams

If you encounter a suspicious email or website that says it's from Islanders Bank, do not respond to it or click any links.

What to do

Never open attachments, click on links, or respond to emails from suspicious or unknown senders. If you receive a suspicious email that appears to be from Islanders Bank, forward the email to mybank@islandersbank.com

What is Phishing

Phish or fraudulent emails may contain links to phony websites or request you to share personal or financial information by using words, such as "Urgent", or "Cancelled", for example, an urgent need to update your information to ensure the security of your records.

Phishing is usually a two part process the fraudsters, also known as phishers, send out a wide audience email that appears to come from a reputable company and this is the phish email.

In the phish email there are links to spoof websites that look and feel like a reputable company's website. Fraudsters are hoping to convince you to share your personal information by using compelling words, such as an "Urgent" need for you to update your information immediately in order to secure your records with the company.

Be very cautious on emails that request you to click on a link to verify your identity, activate an account online or the need to update personal information. Once your personal information is obtain by a fraudster it can be used to open accounts elsewhere in your name, obtain credit in your name, etc.

Fraudulent Websites

Fraudsters will attempt to direct you to a spoof website via emails, text messages, or pop-up windows. These websites are used to obtain your personal information.

How do you detect a phony website? Consider how you got to the website; use caution if you followed the link from a suspicious email, text message or pop-up. Online chatting is another way fraudsters get your personal information.

Pop-up windows are usually ads or small windows to obtain personal information. They generally show up after downloading free downloads such as screen savers.

Text Messages are sent to mobile devices and are called smishing, the purpose of smishing is the same as phishing emails to convince you to share your personal information.



Bank Account, Credit Card and Debit Card Security Tips

Bank Account Security Tips

- Report lost or stolen cards and checks immediately.
- Limit the amount of information on checks. Don't put your Social Security Number or your Driver's License number on your checks.
- Carry your checkbook with you when necessary.
- Store new and cancelled checks in a safe and secure location.
- Review your account statements carefully. Regular viewing of your account statements helps to detect and stop fraudulent activity.

Credit Card and Debit Card Security Tips

- Report lost or stolen cards immediately.
- Always keep your credit or debit card in a safe and secure place.
- Do not give out your card number over the phone unless you initiated the call.
- Do not send your card number through email.
- Do not write your PIN on the back of the card, nor have it written down somewhere in your wallet/purse where your card is located. Memorize it!
- When selecting a PIN don't use any numbers or words that are located in your wallet.
- Ensure no one sees your PIN when you enter it.
- Cancel and cut up unused Credit/Debit cards.
- If you receive a replacement card, destroy your old card.
- Shop with merchants you know and trust.
- Make sure any internet purchase activity you engage in is secured with encryption to protect your account information. Look for "secure transaction" symbols like a lock symbol in the lower right or left hand corner of your web browser window, or https://... in the address bar of the website. The "S" indicates "Secure" and means that the web page uses encryption.
- Always log off from any website after a purchase transaction is made from your Debit or Credit Card. If you can't log off then shut down your browser to prevent unauthorized access to your account information.
- Dispose of your transaction receipts properly.

Using your card at an ATM

- Report all crimes immediately to the operator of the ATM or local law enforcement.
- Be aware of your surroundings and use caution when withdrawing funds.
- Consider having someone accompany you when using an ATM after dark.
- Ensure no one sees your PIN when you enter it.
- Watch for suspicious persons or activity around the ATM. If you notice anything out of the ordinary, either come back later or use an ATM elsewhere. If you observe suspicious persons or circumstances, do not use the ATM at that time. If you are in the middle of the transaction at the time, cancel the transaction, take your card and leave the area.



Using your card at an ATM, cont.

- Skimming devices are often false panels attached to the ATM—usually where the card inserts into the machine. Wiggle the card swiper and any other parts of the ATM that look damaged or different to check for looseness. Also look for new or suspiciously placed cameras and unusual signage.
- Put your cash away as soon as your transaction is complete. Wait to count cash when it is safe to do so.
- Safely keep or dispose of your ATM receipts.

Preventing Credit and Debit Card Fraud

- Never leave receipts behind where someone could pick them up for example at gas stations, ATM's and supermarkets.
- Do not put your debit card account number on your check or any document not associated with a purchase on your account.
- Store your credit/debit card in a secure place where you will immediately know if it is missing.
- Sign the back of your credit/debit card as soon as you receive it.
- Never leave your credit/debit card as a “security deposit” or as identification.
- Never lend your credit/debit card to anyone.
- When you are expecting a new or replacement credit/debit card in the mail keep an eye out for it in the mail.
- Report Lost/Stolen credit/debit cards immediately.
- Never carry your PIN or write your PIN on the back of the card.
- Never choose a PIN that is obvious, such as birth date or telephone number or a set of numbers or words that are located in your wallet.
- When traveling only carry cards that you will use, make copies and place in a safe place so if you need to report which cards are missing or need the Lost/Stolen phone number you have a copy.
- When traveling consider purchasing a re-loadable travel debit card instead of using your debit card that is linked to your checking account.
- When traveling consider using cash for the smaller merchants and items over using your debit card. Use your debit card at well know merchants while traveling.
- Limit your use of foreign ATM's, instead of making several small withdrawals each day, make a couple of big withdrawal's every 3 days or so.
- Be cautious of your surroundings when using a foreign ATM and check for loose components on the front of the ATM or for small pin size camera's trying to capture you entering your PIN.
- Dedicate one credit/debit card for traveling or purchases online for the ease of keeping track of transactions.

General Fraud Prevention Tips

- Be protectful of your personal information; carry only necessary information with you.
- Leave items like unused credit/debit cards and your social security card at home in a secure and safe location.
- When traveling consider purchasing a re-loadable travel debit card instead of using a debit card that is attached to your checking account.



General Fraud Prevention Tips, cont.

- Do not provide your Social Security Number unless absolutely necessary.
- Don't respond to suspicious ("phishing") emails.
- Beware of Suspicious ("spoofing") websites
- Keep your personal computer updated with anti-virus definitions and patching.
- Don't share personal information on social networking sites
- Replace paper statements, invoices with electronic versions.
- Shred documents containing personal or financial information before discarding. Most fraud and identity theft is from mail or garbage theft.
- Avoid downloading files from unknown sources
- Always verify you are on a secure site. A secure site begins with "https" rather than "http".
- Place outgoing mail in a U.S. Postal Service mailbox to reduce the chance of mail theft.
- Retrieve your mail in a timely fashion in order to limit the opportunity for theft.
- Know your billing and statement cycles. Contact the company's customer service department if you stop receiving your regular billing or statement.
- Once a year review your credit report to look for unknown or suspicious transactions. You can get a free credit report once a year from each of the three major credit bureaus at www.annualcreditreport.com.