Digital Banking Security

Barwick Banking Company works hard to ensure the security of our systems and your information. You can be assured that your information is safe at Barwick Banking Company but there are steps you can take to help protect yourself against fraudulent activity.

How to Protect Yourself from ID Theft

- Report lost or stolen cards immediately.
- Shred all materials in a home shredder that have important information on them such as your full name, date of birth, account numbers, etc. Individuals have had their identities stolen from "dumpster divers".
- Never share your full Social Security number with any one through email. Email is not a secure method of transferring confidential information of ANY kind.
- Check your credit report at least annually to dispute any possible discrepancies. You can obtain a free yearly credit report here: Annual Credit Report

Our Promise

Barwick Banking Company will NEVER contact you through email for confidential information such as your account number or Social Security number. If you receive such an email from us please call us immediately to notify us as this is a common tactic known as "phishing". If we need to update such information about you, we will contact you through more secure methods.

For more information on ID Theft please visit Federal Trade Commission.

Barwick Banking Company's Commitment to Security

Barwick Banking Company will NEVER request personal information by email or text messaging including account number, passwords, personal identification information or any other confidential customer information. Fraudulent emails may be designed to appear as though they are originated by Barwick Banking Company. Do not respond to any email communications that requests any type of personal or confidential information and do not go to any links listed on that email. Emails of this nature are not originated by Barwick Banking Company. Never give out any information that the bank already has to any caller, texter, or email sender. If you contact us, we may verify the last 4 digits of your SSN to confirm your identity, but we will never contact you and ask for your debit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal confidential information and we work diligently to do so. We always work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible. We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.

Suspicious Emails or Websites

IMMEDIATELY REPORT ANY SUSPICIOUS EMAILS OR WEBSITES TO BARWICK BANKING COMPANY.

If you suspect identity theft or have any questions regarding this notice, please contact Barwick Banking Company.

Internet Products and Services

1. Secure Login ID and Password or PIN
    a. Do not disclose Login ID and Password or PIN.
    b. Do not store Login ID and Password or PIN on your computer.
    c. Regularly change password or PIN and avoid using easy-to-guess passwords such as names or birthdays. Password should be a combination of characters (uppercase and lowercase) and numbers and should be at least 8 characters in length.
2. Keep personal information private.
    a. Do not disclose personal information such as address, mother's maiden name, telephone number, social security number, bank account number or email address -- unless the one collecting the information is reliable and trustworthy.
3. Keep records of online transactions.
    a. Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
    b. Review and reconcile monthly credit card and bank statements for any errors or unauthorized transactions promptly and thoroughly.
    c. Check email for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
    d. Immediately notify the bank if there are unauthorized entries or transactions in the account.
4. Check for the right and secure website.
    a. Before doing any on line transactions or sending personal information, make sure that correct website has been accessed. Beware of bogus or "look alike" websites which are designed to deceive consumers.
    b. Check if the website is "secure" by checking the Universal Resource Locators (URLs) which should begin with "https" and a closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site.
    c. Always enter the URL of the website directly into the web browser. Avoid being redirected to the website, or hyperlink to it from a website that may not be as secure
    d. If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions online.
5. Protect personal computer from hackers, viruses and malicious programs.
    a. Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs.
    b. Ensure that the anti-virus program is updated and runs at all times.
    c. Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.
    d. Always check with an updated anti-virus program when downloading a program or opening an attachment to ensure that it does not contain any virus.
    e. Install updated scanner software to detect and eliminate malicious programs capable of capturing personal or financial information online.
    f. Never download any file or software from sites or sources, which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to a computer virus that could hijack personal information, including password or PIN.

6. Do not leave computer unattended when logged-in.
    a. Log-off from the internet banking site when computer is unattended, even if it is for a short while.
    b. Always remember to log-off when e-banking transactions have been completed.
    c. Clear the memory cache and transaction history after logging out from the website to remove account information. This would avoid incidents of the stored information being retrieved by unwanted parties.
7. Check the site's privacy policy and disclosures.
    a. Read and understand website disclosures specifically on refund, shipping, account debit/credit policies and other bank terms and conditions.
    b. Before providing any personal financial information to a website, determine how the information will be used or shared with others.
    c. Check the site's statements about the security provided for the information divulge.
    d. Some websites' disclosures are easier to find than others - look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If the customer is not comfortable with the policy, consider doing business elsewhere.
8. Other internet security measures:
    a. Do not send any personal information particularly password or PIN via ordinary e-mail
    b. Do no open other browser windows while banking on line.
    c. Avoid using shared or public personal computers in conducting eBanking transactions.
    d. Disable the "file and printer sharing" feature on the operating system if conducting banking transactions online.
    e. Contact the banking institution to discuss security concerns and remedies to any online e-banking account issues.

ATMs and Debit Cards

1. Use ATMs that are familiar or that are in well-lit locations where one feels comfortable. If the machine is poorly lit or is in a hidden area, use another ATM.
2. Have card ready before approaching the ATM. Avoid having to go through the wallet or purse to find the card.
3. Do not use ATMs that appear to have been tampered with or otherwise altered. Report such condition to the bank.
4. Memorize ATM personal identification number (PIN) and never disclose it with anyone. Do not keep those numbers or passwords in the wallet or purse. Never write them on the cards themselves. And avoid using easily available personal information like a birthday, nickname, mother's maiden name or consecutive numbers.
5. Be mindful of "shoulder surfers" when using ATMs or POS terminals. Stand close to the ATM/POS and shield the keypad with hand when keying in the PIN and transaction amount.
6. If the ATM is not working correctly, cancel the transaction and use a different ATM. If possible, report the problem to the bank.
7. Carefully secure card and cash in the wallet, handbag, or pocket before leaving the ATM or POS terminal.
8. Do not leave the receipt behind. Compare ATM receipts to monthly statement. It is the best way to guard against fraud and it makes record-keeping easier.
9. Do not let other people use your card. If card is lost or stolen, report the incident immediately to the bank.