

ONLINE SECURITY	2
TYPES OF FRAUD	2
Phishing	2
Pharming	2
Credit Card Fraud	2
Phone Solicitations	2
Print Fraud	3
Check Scams	3
Mail Fraud	3
EXAMPLES OF FRAUD	3
Phone Scam	3
Sweepstakes or Lotteries	3
Phishing emails	3
Notification of Changed Email Address or Password	3
Request to Update Your Account	4
National Bank of Dominica System/Technical Updates	4
Phone Solicitations	4
HOW TO REPORT FRAUD	4
Help Protect yourself from Becoming a Victim of Fraud or Identity Theft	4
Identity Theft.....	4
Online Fraud.....	5
Credit Card Fraud	5
Check Scams	6
Mail Fraud.....	6

ONLINE SECURITY

Don't get hooked

Be on the lookout for phishing emails that appear to come from National Bank of Dominica. These fraudulent emails may tell you to update or confirm your account information as a result of a security update, technology upgrade, or routine maintenance.

National Bank of Dominica will never trade, rent, or sell your personal information including email addresses to anyone. For more information on our privacy policy, visit our [Privacy](#) section on this National Bank of Dominica Web site.

TYPES OF FRAUD

Phishing

Criminals use fraudulent emails (known as phishes) or pop-up Web pages that appear legitimate and are designed to deceive you into sharing personal or account information. The phishes often include logos of legitimate companies, content from their Web sites, and names of real employees.

Many scammers randomly generate an email address, that's why you may have received fraudulent emails that appear to be from banks you do not have an account with. They may also obtain email addresses online from Web pages, chat rooms, online auctions, directories or other sources.

Remember, National Bank of Dominica will never send unsolicited emails asking customers to provide, update, or verify personal or account information, such as passwords, account numbers, PIN's, credit or Debit Card numbers, or other confidential information.

Pharming

Pharming occurs when you type in a Web address and it redirects you to a fraudulent Web site without your knowledge or consent. The Web site will try and look similar to the legitimate site in hopes of capturing your confidential information.

Credit Card Fraud

Credit Card fraud can occur when someone takes your card and uses it without your consent. It can also happen when the card sits safely in your wallet.

Phone Solicitations

Scammers will attempt to randomly call people with hopes to lure them with cash gifts or prizes in exchange for personal or account information.

Print Fraud

Scammers will use local newspapers publishing fake advertisements with special rates and offers. If clients call, they are asked for their personal information and for an advance payment before the transaction can be completed.

Check Scams

Scammers will overpay for an item purchased and ask the difference to be wired back. Most times the check or card was counterfeit, stolen or forged for a higher amount.

Mail Fraud

Mail fraud occurs when scammers illegally intercept your mail or when you receive unrealistic offers.

EXAMPLES OF FRAUD

The following are examples of fraud that we've identified. We've categorized the scams by their subject matter and content. This page will be updated frequently. Please visit this page often to learn about the latest alerts.

Phone Scam

Scammers call clients stating they are National Bank of Dominica employees in the Bank Customer Support Unit. Scammers claim customer's accounts have been compromised and in order to "secure" their accounts, customer's need to provide them with information about their accounts. If you have concerns about your account, please contact a National Bank of Dominica Customer Support Representative at (767) 255-2647/2652 or (767) 255-2653/2654 or (767) 255-2648/2651/2649/2650.

Sweepstakes or Lotteries

Beware of other lottery scams – especially those that originate from foreign countries via email. Emails notifying you that you've won a lottery or sweepstakes may require you to send money to secure your winnings. These "official" notices sometimes include fake checks. These notifications and checks are fraudulent.

Phishing emails

Take care when clicking on links within emails – phishing emails may appear to be from legitimate companies. See examples [above](#).

Notification of Changed Email Address or Password

Fraudulent emails notifying clients of changes to their email addresses or passwords have been identified. The emails include statements such as: "Thank you for banking online at National Bank of Dominica.com. Our records indicate that you recently added or made a change to one of your email address(es). This notification is to confirm that you initiated this change. If you feel you have received this email in error and did not add or change your email address(es), please click here."

This email is not from National Bank of Dominica Ltd. and is fraudulent. Users should not click on the link in these emails; the link may take them to a phishing site or could download spyware to their computers.

Request to Update Your Account

Some users have received emails stating they need to update their National Bank of Dominica account "due to the recent changes we have made on Bank-**a-Net**" which "allows us to activate new features for your account on our system." The email includes a hyperlink that appears to take users to a National Bank of Dominica Web site. However, the hyperlink takes users to a phishing site or can download spyware to their computers.

This email is not from National Bank of Dominica and is fraud.

National Bank of Dominica System/Technical Updates

Many fraudulent emails mention "system", "technical", or "technology" updates at National Bank of Dominica. For example, one email tells clients that there has been a "regular update and verification" to their accounts, and that they need to verify their information. Customers are warned that their access to Bank-**a-Net** will be limited if they do not respond.

Phone Solicitations

"Gift of \$10,000 cash" the caller tells clients that they've won a gift of \$10,000. Customers are asked to confirm their account and routing numbers so that the money can be transferred to their accounts by wire transfer.

Customers receive a voice mail and are asked to verify possible fraudulent activities on their cards. The voice mail includes bogus phone numbers for clients to call.

HOW TO REPORT FRAUD

- To report a suspicious email, Web page, or phone call, forward information about the email or Web page to customersupport@nbd.dm
- If you believe you have provided personal or account information in response to a fraudulent email, Web site, or phone call, immediately contact a National Bank of Dominica Customer Support Representative at (767) 255-2647/2648 or complete the "Online Fraud Form."

Help Protect yourself from Becoming a Victim of Fraud or Identity Theft

There are many things you can do to help secure your identity and your accounts. Here are some tips to follow.

Identity Theft

- Don't leave incoming mail lying around.
- Drop your mail in an official postal mailbox.
- Shred or destroy any junk mail before you throw it away.
- Don't respond to unsolicited requests for personal or account information.
- Use a safe deposit box to protect important documents.

Online Fraud

- Look beyond the logo. To make fraudulent emails or Web sites appear real, scammers often include actual logos and images of legitimate companies. They also convey a sense of urgency, stating that if you fail to provide, update, or verify your personal or account information, access to your accounts will be suspended. It's important that you look beyond the logo and not give out your information.
- Use your spam filter. Many email services now have spam filters that minimize the amount of spam you receive. The filters can help you minimize the number of fraudulent emails in your inbox.
- Type, don't click. Even if you do open a suspicious email, don't click on any links. By clicking on the links, you could unknowingly download a virus or spyware to your computer. Even if you think the email is legitimate, type Web addresses into your browser instead of clicking on links. If the email is from an institution you do business with, use a bookmark that you've already created to visit the company's Web site.
- Change your online passwords often. The rule of thumb is to change your password every 30 to 60 days. Be creative with your passwords – stay away from obvious passwords like your ZIP code, year of birth, or sensitive information such as your mother's maiden name or your Social Security number. Include numbers and letters so passwords can't be easily intercepted or guessed by others.
- Update your anti-virus and anti-spam software. By keeping anti-virus and anti-spam software up to date on your computers, you make it more difficult for scammers to access your personal and account information. You can purchase anti-virus and anti-spyware software at retail stores, as well as on the Internet.
- Delete emails from unknown senders.

Credit Card Fraud

- Sign your cards immediately once they arrive in the mail.
- Memorize your PIN and don't write it on anything.
- Don't enter your card online unless you're on a secure site. Don't send your credit card number in the mail.
- Keep a record of all your account numbers, expiration dates, and contact information for each issuer. This will come in handy if your wallet is lost or stolen.
- Report a lost or stolen card right away to your Bank. Quick action will minimize potential loss and liability.
- Save your receipts to compare against your billing statement. When discarding receipts, tear them up or shred them.

- Monitor your statements monthly, making sure you recognize all charges. If you see any suspicious transactions, contact your Bank immediately.
- Carefully review receipts for voided transactions and be sure they do not post to your account.
- Destroy your carbons. Do not leave them behind without tearing them up.
- Don't leave your purse, wallet, cards, or receipts unattended. Always keep them secure or in your sight.
- Only carry cards that you need; leave others in a safe place at home.
- Don't give out your card account number unless you know and trust the company.
- Shield your hand from view of others when entering your PIN at ATMs.

Check Scams

- Use Direct Deposit for paychecks, Social Security payments, and other regular deposits.
- Be aware of fake check scams that promise easy money, winning sweepstakes, or depositing checks from foreign countries.
- Do not leave your checkbook unattended.
- Know who you are doing business with.
- Report lost or stolen checks immediately to National Bank of Dominica by calling (767) 255-2648/2649

Mail Fraud

- Shred documents containing your personal and financial information before placing them in the trash.
- Report any unauthorized transactions to the Customer Support Unit at (767) 255-2648/2649 immediately.