# Fraud & Identity Theft Prevention Tips

## Important Information for You

We're providing the tips below to help you and your loved ones learn more about fraud and identity theft

**Please note:** Down East Credit Union will never ask you to provide personal or account information via email.

## Steps to Prevent and Reduce the Risk of Fraud and Identity Theft

### What to do if your card is lost or stolen

Please contact Down East Credit Union immediately at 1-800-427-1223 or call 1-800-472-3272 after hours to block your debit or credit card.

### Don't Give Out Too Much Information

The first and easiest precaution is to not share too much information about yourself. Before posting anything on websites like Facebook or Twitter, determine if it could be used to gain access to any of your confidential information—such as financial accounts, your personal email account or even online accounts for your cell phone and other utilities.

### Protect Your Home Wireless Network

The less protected your home wireless network is, the more vulnerable you are to identity theft. Here are a few steps you can take to help ensure your personal information isn't being shared with the neighborhood—or a hacker.

1. Turn on encryption on your wireless router. If your router does not allow encryption, replace it. The extra cost is worth the extra protection.
2. On your computers, implement anti-virus and anti-spyware software and a firewall. This is very important when using public wireless networks.
3. If your router allows identifier broadcasting, turn it off. You know the network exists; there is no need to broadcast it for everyone to see.
4. Change the default identifier on your router so that it is not the standard used by the manufacturer. Hackers know standard manufacturer IDs.
5. Change the router's preset password. Hackers know these preset passwords. Use a strong password—long and not easily guessed.

### Passwords—Be Sure they are Secure

Many websites require a User ID and Password for access, so we don't want to make the mistake of creating a password that is too easy for others to figure out. Take a look at a few tips for creating passwords:

1. Passwords should be at least 8 characters long.

2. Try to use a combination of lower case letters, upper case letters, numbers and special characters (if they're allowed by the website).
3. Try to create a string of characters that will be easy for you to remember, but not for someone else to guess.
4. Avoid using school names, birthday and anniversary dates and the names of loved ones or pets.

# Phishing & Spoofing Prevention

Never click on the link provided in an email you don't fully trust. Remember, sometimes your friends and family get "spoofed" and generate emails that propagate viruses to other computers.

Do not open an attachment to an unsolicited email, unless you have verified the source, and you are comfortable that the source actually sent it.

Do not be intimidated by an email or caller who suggests dire consequences if you do not immediately provide or verify information. Remember, Down East Credit Union never asks members for ATM passwords or Online Banking/Down East account access codes.

If you believe the contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the email.

Use the FTC (Federal Trade Commission) website, onguardonline.gov to learn more. Consumers can take interactive quizzes designed to enlighten them about identity theft, phishing, spam and online-shopping scams. Elsewhere on the site, consumers can find detailed guidance on how to monitor their credit histories, use effective passwords and recover from identity theft.

# Smartphone Security

Smartphones are used for everything from obtaining information at the drop of a hat to accomplishing daily tasks. It works great and provides convenience, but, as with other technology, some simple rules should be followed to limit your exposure to identify theft and other fraud:

1. Keep your phone's operating system secure. This is particularly important with Android™ systems and other open systems. Closed systems, such as Apple's iPhone®, screen and approve apps before they are published, but open systems do not. With an open system, you may want to purchase a security tool, such as Lookout™ Mobile Security or Norton™ Mobile Security for Android™ phones.
2. Keep an eye on your phone's behavior. If your phone starts to act differently—somewhat erratic or funny—take it to a technician for an inspection. Malware (short for malicious software) can cause things to look or act differently, and watching for red flags may catch suspicious activities before they can do some damage—like transmitting identity information.
3. For Android™ users, it's best to read the list of permissions that an app requests before you install it. Do these permissions make sense for the app you purchased? An example

may be a game that requests permissions for SMS (Short Message Service) texting or access to your contact list. Does the game really need these permissions?

4. Read the fine print when subscribing to services, and stay alert to links you are accessing.
5. Do not click on an email or SMS link unless you know the email or text is from a valid and trusted source. Just like email on your computer, links to fraudulent sites can be disguised in what appear to be valid sources, exposing you to identity theft or fraudulent purchases.
6. If you ever suspect that your account at Down East CU—or any other organization—has been exposed or compromised, contact that organization immediately.

This post is not intended to provide technological or security advice. Contact your authorized service provider for details of your service agreement and consult with a technology support service for questions related to Smartphone security. Down East does not endorse or recommend any of the products or services represented herein.

# Information for Victims of Identity Theft

If you are a victim of identity theft, the following four steps should be completed as soon as possible. Be sure to keep records and details of conversations and correspondence.

1. Place a fraud alert on your credit reports and review your credit.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.
3. File a complaint with the Federal Trade Commission.
4. File a report with your local police or the police in the community where the identity theft took place.

Information from https://www.consumer.ftc.gov/features/feature-0014-identity-theft. Please visit this site for more details.

# Glossary

**Card Scanning/Skimming**
A device used to scan and save information from credit cards, drivers licenses, passports, medical cards and other laminated cards. Unfortunately, these devices are readily accessible to buy online.

**Data Breach**
The unintended disclosure of information that compromises the security of personal information, and can often lead to instances of identity theft.

**Drive-by Download**
Software that secretly and automatically installs on your computer when you visit certain websites. The user is usually unaware that anything was installed until after the fact.

**Fraud**
Any act or practice resulting in the loss of someone’s rights or property. It usually involves making false and misleading representations with the intention of cheating or stealing from another person.

**Hacker**
Someone who exploits security holes in technology for any purpose.

**Hidden Dialers**
Programs that can use your computer to dial expensive phone calls that later show up on your phone bill

**Identity Fraud**
Identity fraud is different from identity theft. ID fraud is using personal information that is made up rather than stolen from a real person.

**Identity Theft**
Identity theft occurs when a thief steals someone else's personal information as his own, creating a new identity of an existing person. Some ID theft items can include a social security number, driver's license number, usernames and passwords, employee ID number, mother's maiden name, and account information, including bank and credit union account

**Keystroke Logging**
A software development tool that captures the user's keystrokes. Its intended use is to measure employee productivity on clerical tasks. Keylogging has been abused by individuals who can easily buy the tool to spy on computers and obtain passwords or encryption keys.

**Mail Fraud**
Thieves steal paper mail from your mailbox to obtain personal information, pre-approved credit card applications, medical insurance statements or any other information that will help them get credit in your name.

**Malware**
Short for "malicious software," it refers to any harmful software. Malware includes computer viruses, worms, Trojan horses, and also spyware.

**Pharming**
Hackers redirect internet traffic from one website to a different, identical-looking site in order to trick you into entering your username and password into the database on their fake site. Your computer or DNS server has been hijacked into going to the fake site.

**Phishing**
Thieves trick someone into giving them confidential information, usually through links within emails sent to the user falsely claiming to be a legitimate business or company in order to scam the user into giving private information. In most cases, these emails appear to come from financial institutions.

**Pretexting**
Thieves collect individual's personal information under false pretenses such as posing to be from a charity or other legitimate organization. This is typically done over the phone or via email.

**Security Alert**
A statement added to one's credit report when a credit bureau is notified that the consumer may be a victim of fraud. It remains on file for 90 days and suggests that creditors should request proof of identification before granting credit in that person's name. Once a security alert is in place, the report is no longer available for online viewing.

**Spam**
Unsolicited commercial emails. Many of these come from legitimate companies but many also come from questionable businesses.

**Spoofing**
A fraudulent website or email that appears to be from a well-known company and attempts to get you to provide, update or confirm personal information. Similar to pharming.

**Spyware**
General term for any technology that gathers information about a person or organization without their knowledge. Advertisers or other interested parties often use spyware programming to gather and relay information.

**Trojan Horses**
Unlike a virus, Trojan horses contain or install malicious programs that can run autonomously, masquerading as a useful program, or hack into the code of an existing program and executes itself while that program runs.

**Viruses**
Malicious programs with the ability to replicate and install themselves, or infect, a computer without the computer user's knowledge or authorization. Viruses are often unintentionally downloaded when the user accidentally clicks on a link to a virus.

**Vishing**
Using Voice over Internet Protocol (VoIP) phone numbers to steal user information.

**Worms**
Computer viruses which can self-replicate by resending themselves via email or a network message.

*Information from [http://www.identitytheft.com](http://www.identitytheft.com)*