Essentials

Select Saversclub
AN AFFILIATE OF QUORUM FEDERAL CREDIT UNION

WHERE GOOD SENSE MAKES GOOD MONEY.

THIS NEWSLETTER IS PUBLISHED QUARTERLY FOR MEMBERS OF SELECT SAVERS CLUB.

Welcome to the Select Savers Club!

The Select Savers Club (SSC) is a not-for-profit club designed to educate and empower its members with financial knowledge. We are committed to helping our members achieve their financial goals with information on spending, saving, borrowing, and managing money and debt wisely. Membership is open to anybody with a desire to learn about financial matters, savings and the wise use of credit.

AT A GLANCE

Meeting of the Membership

November 17, 2021
1:00 - 1:30 p.m. ET
Virtual Board Room
RSVP: info@selectsavers.org

USEFUL WEBSITES

- SelectSavers.org
- PracticalMoneySkills.com
- FTC.gov
- quorumfcu.org

CONTACT INFORMATION

Telephone
914.641.3765

Email Address
info@selectsavers.org

Mailing Address
Select Savers Club
P.O. Box 566
Purchase, NY 10577-0566

BOARD OF DIRECTORS

- Dave A. Peart
- Caryl Buhler
- Sharon Cobo
- Andrew Chunka

ISSUE DATE: November 2021

5 Steps to Take After a Data Breach

According to Risk Based Security's Mid-Year Data BreachReport, there were 1,767 publicly reported breaches in the first half of 2021, exposing 18.8 billion records. One of the most far-reaching of these breaches was the T-Mobile data breach in August, which impacted more than 50 million people. A data breach exposes confidential information of its victims, which can include Social Security numbers, account information, credit card numbers, passwords and more. If your personal information has been compromised, take these five steps to mitigate the damage.

1: Read all notifications from the compromised company.

The business whose data has been compromised in the breach will generally reach out to all potential victims to notify them about the exposure. They may instruct all recipients to check for signs that their information has been exposed and/or direct them toward their next step. If you believe your information may have been compromised in a breach, it's important to read every message you receive from the exposed company.

2: Alert your financial institution.

Next, let your financial institution know your account may have been compromised. This way, they'll know to keep an eye out for signs of fraud and place an alert on your account. They'll be watchful of requests to approve any large transaction or withdrawal, and will contact you if they notice any suspicious activity.

3: Change any exposed passwords.

A data breach can sometimes mean that more than one of your passwords has been compromised. It's best to change as many as possible after a breach to keep information and money safe. The quickest way to do this is by using a password manager, which allows you to store unique, complex passwords for each account. Although it's important to have a different password for each account, it's best to start by changing passwords you know were a part of the data breach.

4: Consider a credit freeze.

A credit freeze alerts lenders and credit companies that you may have been a victim of fraud. This added layer of protection will make it difficult, or impossible, for hackers to open a new credit line or loan in your name. You can freeze your credit at no cost with all three of the major credit bureaus, Equifax, Transunion and Experian. You'll need to provide some basic information and you'll receive a PIN for the freeze. Use this number to lift the freeze when you believe it is safe to do so.

5: File an identity theft report.

If your accounts have been compromised and you believe your identity has been stolen, file an identity theft report with the Federal Trade Commission (FTC) immediately. This will assist the feds in tracking down the scammers responsible for the data breach. It will also help you return your finances to their usual state as quickly as possible. Take these precautionary measures to protect your information from future data breaches:

• **Monitor your credit**. It's a good idea to check your credit accounts for suspicious activity on a regular basis. You may also want to sign up for credit monitoring, a service that will cost you $10-40 a month for the promise of notifying you immediately about any suspicious activity on your accounts.

• **Use strong, unique passwords**. Use a different password for each account, and choose codes that are at least eight characters long. Use a variety of numbers, letters and symbols–and vary your capitalization use as well. Choose two-factor authentication when possible, and non-password authentication, such as face recognition or fingerprint sign-in, for stronger protection.

• **Browse safely**. Never share sensitive information online and always keep your security and spam settings at their strongest levels.

These strategies can reduce your energy expenses in summer without sacrificing comfort. Making these simple changes also preserves natural resources and may help prevent summer brownouts by curbing demand on the energy supply.