Cybersecurity Incident

On September 7, 2017, Equifax, one of the three major credit bureaus reporting agencies in the U.S. announced that on July 29, 2017, a data security incident occurred potentially exposing consumers' personal information. The information accessed includes names, Social Security numbers, date of birth, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers were accessed. Equifax has since reported the incident to law enforcement agencies and is working with authorities

This cyber security incident can potentially impact 143 million U.S. consumers. Equifax has established a dedicated website, www.equifaxsecurity2017.com , to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers – all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visitwww.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559 which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern time.

What can you do to protect yourself?

Below are simple reminders that you can do to help protect your computer from online criminals.

1. Ensure that your Credit Union has current and up-to-date contact information like; address, phone numbers, email address and alternate phone numbers.
2. Have computer security programs running and regularly updated to look for the latest threats.
3. Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information.
4. Get to know standard Internet safety features i.e. https:// at the beginning of the Web address means that the website is authentic and encrypts data during transmission.
5. Ignore unsolicited emails asking you to open an attachment or click on a link if you're not sure it's who truly sent it and why.
6. Be suspicious if someone contacts you unexpectedly online and asks for your personal information.
7. Create strong passwords that are hard to guess, change them regularly and don't use the password or PIN for multiple accounts.
8. Be discreet when using social networking sites.
9. Be careful when using smartphones and tablets. Don't leave your mobile device unattended and use a device password or other method to control access if it's stolen or lost.
10. Talk with your child about being safe online, including the risks of sharing personal information with people they don't know, and make sure the devices they use to connect to the Internet have up-to-date security.