Be Careful about Security Breach Emails

At least one major retailer has sent emails to millions of customers potentially affected by the recent mega security breaches. Be on the lookout for scammers who mimic them (*CNN Money* Jan. 20).

Homeland security investigators have warned several large retailers about sophisticated malware that has potential to compromise customers' credit card numbers and other personal information on an unprecedented scale. Target alone has as many as 110 million affected customers.

While the hacking is under investigation, if you receive email from a retailer regarding a security breach, here's what to do:

Don't automatically open the email: First go to the retailer's website or call to make sure the information online matches the email you received. One adviser, Adam Levin of Credit.com, cautions that even opening a fraudulent email could allow malware to be installed on your computer.

If you've already opened the email: Don't click on any links until you verify the information with the retailer by going online or calling.

If you've already clicked a link to an external website and entered personal information: Verify the information in the email with the retailer at its website. If the information in the email doesn't match the retailer's information, take action quickly:

- If the retailer is offering free fraud-monitoring, take advantage of it. Your credit union also might offer a fraud-monitoring service or recommend an affordable and reliable outside service.
- Check and confirm your debit and credit card transactions every day via your financial institution's online platform.
- Alert your financial institution, the credit card company, and call the "big three" credit reporting agencies--Equifax, TransUnion, and Experian--to tell them you clicked through on a bogus link and shared info you wish you hadn't.
- Ask to have a fraud alert placed on your account. It costs nothing to place a fraud alert on your credit report if your information is compromised, and the alert will remain in place for 90 days.
- Alert the Federal Trade Commission (FTC). Report fraud via FTC.gov or by calling 877-438-4338.
- If you're really worried, request a credit freeze, which prohibits any credit from being extended under your name.

To learn more about protecting your accounts from fraud, talk to the professionals at your credit union. They can recommend steps you can take to keep your information safe.

Source: CUNA