DFCU will never ask you to give your personal and confidential information through an email, text, or voice message. If we initiate contact with you, then we already have this information on record and would have no need to ask you for it.

Phishing Information and Prevention Tips

Phishing

Phishing is the process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity using bulk email which tries to evade spam filters.

Emails claiming to be from popular social web sites, credit unions, banks, retailers, or government agencies are commonly used to lure the unsuspecting public. It is a form of criminally fraudulent social engineering.

The most common form of phishing would be via email. However, text and voice message attempts have become more common, as well. A "spammer" (a term used for these offenders) will send out an email which they create to look almost identical to a legitimate organization. They may use the company logo and create an email address very close to that of the masqueraded organization.

Most of these fraudulent emails will ask you to click on a link to a website that would be almost identical to the masqueraded organization's website, once you have reached that fake website, they may ask you to login using your online banking credentials (username and password) so they can gain access to your accounts and financial assets.

Vishing

Vishing is another form of Phishing attempting to acquire your confidential Credit Union Account information via Phone calls. The caller always impersonates an employee from your Credit Union or Bank. These calls are typically an automated system that leaves a message stating there is a problem with your account and asks that you call back a phone number or visit a website, then asks for your personal account information. As in a phishing scam, if you offer your information, they will be able to access your accounts therefore compromise your financial assets and personal information.

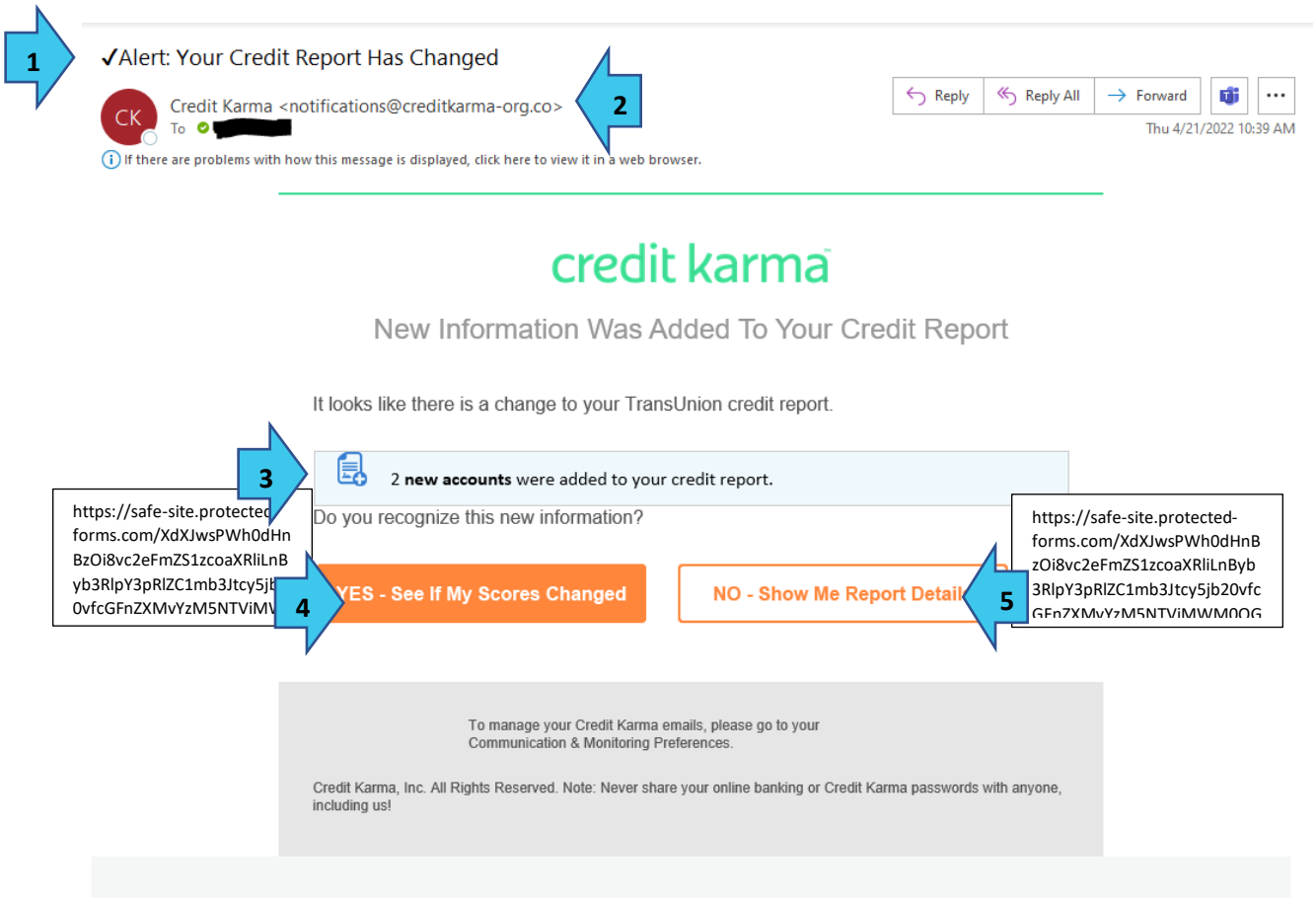
Other forms of scams are via text messaging on your cell phone.

It is important to note that if you do relinquish your information by responding to any of these types of scams you may be liable for any losses incurred to your accounts.

How can we prevent this from happening?

The problem with phishing, vishing, and all similar attempts is that financial institutions, retailers and government agencies cannot directly control it. Scammers are setting up fake sites and emails and sending them out to thousands (in some cases millions) of consumers. The only way information becomes compromised is if receiving party of those spam emails falls prey to the scam and gives out their personal information and credentials.

Since we cannot prevent it from happening, the best way to minimize the impact is through **AWARENESS**. Here are **few tips** to help you identify those spam emails, but first see if you can identify what is wrong with the example email listed below:



Notice the following is suspicious about the email above:

1. The subject line is urging you to act!
2. The sender is claiming to be Credit Karma (a legit company), however the domain name they are using is creditkarma-org.co while the legit domain is creditkarma.com (This is a big red flag)

3. The sender is informing you that there is a change to your credit report but never listed those changes!!
4. The sender is asking you to click for confirmation. Notice: by hovering the mouse over the button it displays a link-to address that is for a different website than legit Credit Karma website. (This is a big red flag)
5. The sender is asking you to deny by click on the No button. Notice: by hovering the mouse over the button it displays a link-to address that is for a different website than legit Credit Karma website. (This is a big red flag)

In conclusion, you have enough red flags to delete this email and if you have any concerns about the email content (on this case your credit report), then you should contact the credit bureaus directly:

- Contact the three major credit bureaus:
  Experian: www.experian.com; credit report copy - 888-397-3742; fraud unit - 888-397-3742
  Equifax: www.equifax.com; credit report copy - 800-685-1111; fraud unit - 800-525-6285
  TransUnion: www.transunion.com; credit report copy - 800-888-4213; fraud unit - 800-680-7289
- Visit the website www.annualcreditreport.com for a free credit report (Please note: one free credit report per year).

A good roll of thumb is to always: